UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GESTIÓN DE BASE DE DATOS III VERSIÓN

TEMA La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior

Trabajo de Investigación previo a la obtención del Grado Académico de Magíster en Gestión de Base de Datos

Autora: Ing. Natalia Judith Crespo Chávez
Director: Ing. Franklin Oswaldo Mayorga Mayorga Mg.

Ambato – Ecuador
2018

A la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por Ingeniera Pilar Urrutia Magister, e integrado por los señores Ingeniero David Omar Guevara Aulestia Magister, Ingeniero Hernán Fabricio Naranjo Ávalos Magister, Ingeniero Félix Oscar Fernández Peña Doctor, designados por la Unidad Académica de Titulación de Posgrado de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: “La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior, elaborado y presentado por la señora Ingeniera Natalia Judith Crespo Chávez, para optar por el Grado Académico de Magister en Gestión de Bases de Datos; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Pilar Urrutia, Mg.
Presidente del Tribunal

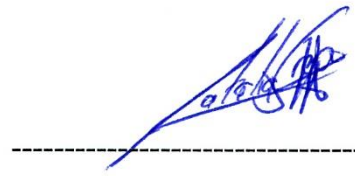
Ing. David O. Guevara A., Mg.
Miembro del Tribunal

Ing. Hernán F. Naranjo Á., Mg.
Miembro del Tribunal

Ing. Félix O. Fernández P., Dr.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior, le corresponde exclusivamente a: Ingeniera Natalia Judith Crespo Chávez, Autora bajo la Dirección de Ing. Franklin Oswaldo Mayorga Mayorga Mg., Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.



Ing. Natalia Judith Crespo Chávez

c.c.0603237116

AUTORA

Ing. Franklin Oswaldo Mayorga Mayorga Mg.

c.c.1802503993

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ing. Natalia Judith Crespo Chávez

c.c. 0603237116

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

AGRADECIMIENTO

A la Universidad Técnica de Ambato y los docentes de la Maestría en Gestión de Bases de Datos por su dedicación y compromiso con la formación académica de profesionales.

A mi Director del trabajo de investigación por su acompañamiento y guía para el desarrollo de este trabajo.

DEDICATORIA

A mi familia y mis hijos por ser la inspiración y apoyo para cumplir las metas que me he trazado.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL / DIRECCIÓN DE POSGRADO
MAESTRÍA EN GESTIÓN DE BASES DE DATOS

TEMA:

La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior

AUTOR: Ing. Natalia Crespo Chávez
DIRECTOR: Ing. Franklin Oswaldo Mayorga Mayorga
FECHA: junio de 2017

RESUMEN EJECUTIVO

La evolución de la tecnología y los medios de comunicación han influido drásticamente en la forma en que las sociedades ejecutan sus procesos y la concepción de sus activos, por lo que en la actualidad es preponderante que toda empresa o institución automatice la información relacionada al giro de su negocio, que le permita un oportuno acceso, manipulación, interpretación y transferencia de datos.

Pero de igual manera ha crecido de manera vertiginosa la inseguridad de un activo de vital importancia para el desempeño de toda organización como es la información, ya sea por negligencia en su uso o por intención de causar daño; por lo que se ha vuelto imperante direccionar esfuerzos a gestionar la seguridad de la misma, evitando pérdidas o alteraciones que impliquen un alto costo de

recuperación. Por ello el reto en la actualidad debe ser el trabajo en la prevención y no solo en recuperar daños ocasionados por incidentes de seguridad.

En este contexto la presente investigación se centra en el análisis de la incidencia de las normas ISO 27001 y 27002 en la seguridad de las bases de datos en las Instituciones de Educación Superior (IES), considerando que estas manejan información de alto valor y sensibilidad respecto a sus operaciones académicas, administrativas y de investigación, por lo que se considera importante determinar el nivel de seguridad de la misma.

El estudio se lo puede desagregar en dos momentos: el primero orientado a determinar el estado de la seguridad de la información en las IES, apoyándose de estudios en otras instituciones de Educación Superior y que se complementa con la realización de una auditoría a la Unidad Técnica de Control Académico de la Universidad Nacional de Chimborazo, con base a los 14 objetivos y 114 controles de seguridad que establecen las normas 27001 y 27002 (aplicada con las normas INEN, traducción idéntica de las normas ISO).

El segundo momento se refiere a la propuesta, sustentada en la aplicación de una norma adicional como es la ISO 27005, que brinda el marco metodológico para que la UNACH formalice la seguridad de sus activos de información con base a la gestión de riesgos, el desempeño de los controles de seguridad (resultado de la auditoría) y la implementación de políticas que normen todo el proceso de gestión de seguridad (gestión de seguridad).

Descriptores: seguridad, confidencialidad, integridad, disponibilidad, ISO, INEN, controles, incidentes, vulnerabilidades, amenazas, riesgos, activos de información.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL / DIRECCIÓN DE POSGRADO
MAESTRÍA EN GESTIÓN DE BASES DE DATOS

THEME:

La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior

AUTHOR: Ing. Natalia Crespo Chávez
DIRECTED BY: Ing. Franklin Oswaldo Mayorga Mayorga
DATE: November 2017

EXECUTIVE SUMMARY

The evolution of technology and the media have drastically influenced the way in which companies execute their processes and the conception of their assets, since at present it is imperative that every company or institution automates the information related to the rotation of its business, which allows timely access, manipulation, interpretation and transfer of data.

But in the same way insecurity has developed for an asset of vital importance for the performance of any organization such as information, whether due to negligence in its use or intention to cause harm; so it has become imperative to direct efforts to manage the secure of it, avoiding losses or alterations that imply a high cost of recovery. Therefore, the challenge at present must be the work in prevention and not only in recovering damages caused by security incidents.

In this context, the present investigation focuses on the analysis the incidence of ISO 27001 and 27002 standards on the security of databases in Higher Education Institutions (HEIs), considering that handle information of high value and sensitivity with respect to their academic, administrative and research operations, so it is considered important to determine the level of security of the same.

The study can be disaggregated into two periods: the first is aimed at determining the state of information security in HEIs, based on studies at other institutions and is complemented by an audit to the Academic Control Technical Unit of the National University of Chimborazo, based on the 14 objectives and 114 security controls established by standards 27001 and 27002 (applied with INEN standards, identical translation of ISO standards).

The second moment refers to the proposal, based on the application of an additional standard such as ISO 27005, which provides the methodological framework for UNACH to formalize the security of its information assets based on risk management, performance of security controls (result of the audit) and the implementation of policies that regulate the entire security management process (security management).

Descriptors: security, confidentiality, integrity, availability, ISO, INEN, controls, incidents, vulnerabilities, threats, risks, information assets.

INTRODUCCIÓN

Capítulo I, denominado EL PROBLEMA DE INVESTIGACIÓN, contiene la información relativa al tema de investigación, planteamiento del problema, contextualización, análisis crítico, prognosis, formulación del problema, interrogantes, delimitación, justificación y objetivos.

Capítulo II, denominado MARCO TEÓRICO, contiene: antecedentes investigativos, fundamentación filosófica, fundamentación legal, categorías fundamentales, hipótesis y señalamiento de variables.

Capítulo III, denominado METODOLOGÍA, contiene: modalidad básica de investigación, nivel o tipo de investigación, población y muestra, operacionalización de variables, plan de recolección de información, y plan de procesamiento de la información.

Capítulo IV, denominado ANÁLISIS E INTERPRETACIÓN DE RESULTADOS, contiene: análisis de los resultados, interpretación de datos, verificación de hipótesis.

Capítulo V, denominado CONCLUSIONES Y RECOMENDACIONES, presenta de forma puntual las conclusiones y recomendaciones del trabajo de investigación, respecto al problema planteado.

Capítulo VI, denominado PROPUESTA, contiene: datos informativos, antecedentes de la propuesta, justificación, objetivos, análisis de factibilidad, fundamentación, metodología, modelo operativo, administración y previsión de la evaluación respecto a la institución donde se aplica dicha propuesta.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema

La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior

1.2. Planteamiento del Problema

1.2.1 Contextualización

La información es poder, y su acceso, manejo e interpretación son el puntal clave para la toma de decisiones en todos los ámbitos de desarrollo del ser humano. De allí que la disponibilidad, confidencialidad e integridad de la misma constituyan pieza clave en la gestión de toda clase de instituciones públicas o privadas.

El valor que tiene la información en el contexto económico, social, político y personal, está directamente relacionado con su vulnerabilidad al latente peligro de alteración o pérdida, existiendo o no la intención para ello. (Gómez, A. 2011. Pg. 31, 32).

Los ataques a los sistemas de información y las pérdidas generadas por ello, obligan a las instituciones a buscar soluciones que permitan garantizar la información que se maneja y su permanencia en el tiempo. (Gómez, A. 2011. Pg. 290, 291).

En nuestro país son constantes los ataques o intentos de ataque a las bases de datos de las diferentes instituciones públicas o privadas con la finalidad de

obtener información sensible de operación de las mismas o con el simple propósito de afectar a las mismas por las pérdidas sufridas. (El Comercio, 2015; El Telégrafo, 2011, 2016).

A nivel local instituciones como el Gobierno Autónomo Descentralizado Municipal de Riobamba han sido víctimas de manipulación no autorizada de sus bases de datos, que han implicado pérdidas millonarias para la ciudad. (El País, 2013; La Hora, 2013).

La Universidad Nacional de Chimborazo también ha sufrido ataques a sus bases de datos, que han implicado esfuerzos y tiempo del talento humano para recuperar información. Torres, E (2017). Oficio interno. Universidad Nacional de Chimborazo (no publicado).

Por ello es fundamental que se adopten medidas de seguridad que permitan garantizar la seguridad de la información preservando su confiabilidad, integridad y disponibilidad.

Como se observa en el Gráfico 1, se considera que la poca experiencia en el manejo de normas de seguridad influye en el nivel de seguridad, aplicación de normativas de seguridad y manejo de planes de contingencia y recuperación de desastres respecto a la información.

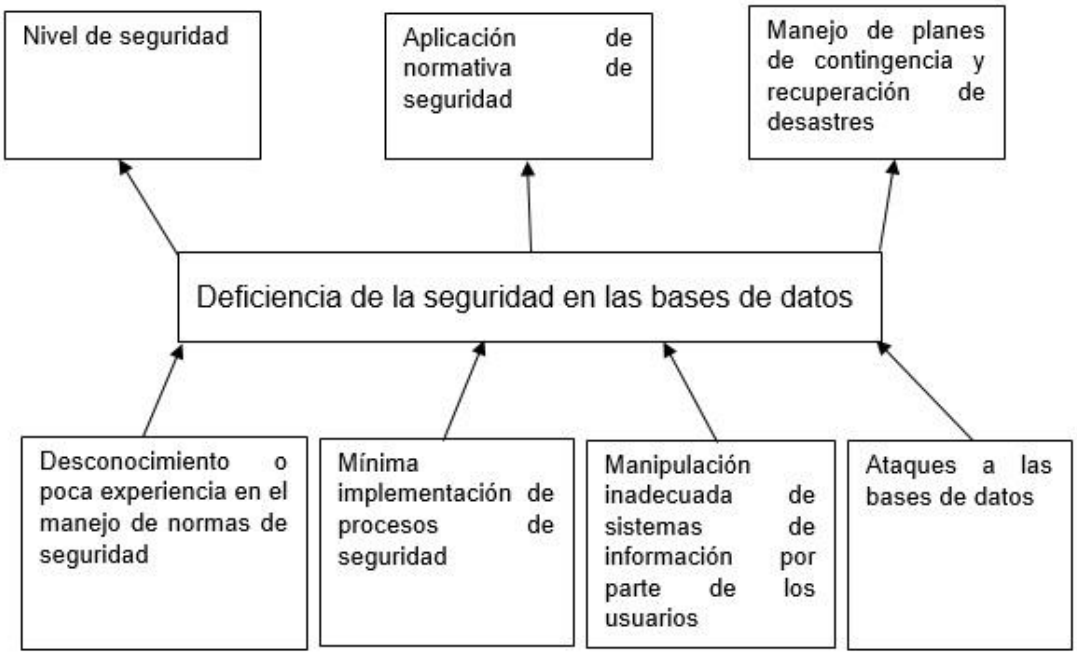


Gráfico 1. Árbol de Problemas
Elaborado por: La Investigadora

1.2.2 Análisis crítico

Considerando que la deficiencia en la seguridad de las bases de datos puede depender de diversas causas como:

- El desconocimiento o poca experiencia en el manejo de normativas en materia de seguridad de información, que favorece la vulnerabilidad de las bases de datos frente a ataques o pérdidas no previstas de datos.

- El mencionado desconocimiento se relaciona con un mínimo desarrollo de procesos de seguridad, que pone en riesgo la confiabilidad, integridad y disponibilidad de la información.

- Un inadecuado manejo de protocolos de seguridad y manipulación de información por parte de los usuarios también pueden poner en riesgo la seguridad de la información.

- Los ataques a las bases de datos también demuestran la deficiencia en la aplicación de normas de seguridad.

Esto desencadena en varios efectos como:

- Altos niveles de inseguridad en las bases de datos por no contar con medidas de seguridad para la información.

- Desarrollo inadecuado de normativas aplicadas a la seguridad de la información por falta de conocimiento del personal encargado de la administración de los sistemas.

- Falta de planes de contingencia y recuperación de desastres que permitan mitigar y controlar una afectación a la seguridad de la información.

1.2.3 Prognosis

En caso de no tomarse acciones correctivas sobre la deficiencia en la seguridad de las bases de datos, la vulnerabilidad de las mismas pondría en riesgo la confiabilidad, integridad y disponibilidad de la información.

Lo antes citado afecta de forma directa al desarrollo armónico de los procesos institucionales y su información académica y administrativa, pudiendo inclusive generar consecuencias de tipo legal, si algún proceso se viera afectado por adulteración o pérdida de datos.

De igual manera la falta de veracidad en la información estadística que debe ser reportada a entidades de control superior, podría desencadenar en llamados de atención o sanciones a la entidad por no garantizar la calidad de información reportada.

1.2.4 Formulación del problema

¿La aplicación de las normas ISO 27001 y 27002 inciden en la seguridad de las bases de datos de las Instituciones de Educación Superior?

1.2.5 Interrogantes (subproblemas)

1. ¿Hay deficiencia en la seguridad de las bases de datos?
2. ¿Ayuda la aplicación de las normas ISO 27001 y 27002 a mejorar la seguridad de la información?
3. ¿Cómo se aplican las normas ISO 27001 y 27002?
4. ¿Se puede proponer una solución factible para la seguridad de las bases de datos?

1.2.6 Delimitación del Objeto de investigación

Delimitación de contenido

Las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos

Campo: Bases de Datos

Área: Escalabilidad de Bases de Datos

Aspecto: Seguridad

Delimitación Espacial: Universidad Nacional de Chimborazo – Unidad Técnica de Control Académico

Delimitación Temporal: de febrero a julio 2017

1.3 Justificación

Se plantea la realización de la presente investigación considerando la importancia de la seguridad de la información requerida para las bases de datos institucionales.

Cada vez es más imperante la necesidad de implementar estándares que garanticen un activo tan importante para toda institución como es la información.

A medida que crecen las vulnerabilidades y peligros potenciales de pérdida de información, por ataques o manejo inadecuado de los sistemas de información, es fundamental que la universidad cuente con políticas que permitan prevenir, controlar y mitigar los riesgos sobre su seguridad, garantizando la disponibilidad, confiabilidad e integridad de la misma.
Esto permite a sus usuarios, disponer de la misma para la ejecución de los procesos académicos y administrativos, así como la toma de decisiones para los procesos de planificación institucional.

La implementación de la normativa y procedimientos de seguridad es de gran utilidad para la institución, ya que permite garantizan la veracidad de información que se maneja así como su permanencia en el tiempo.

Técnicamente es factible por cuanto existe la norma que determina como se debe gestionar la seguridad de la información.

Tiene factibilidad operativa por cuanto es realizable y se enmarca dentro de las necesidades institucionales.

Y tiene factibilidad económica por cuanto se cuenta con la infraestructura necesaria para su estudio y aplicación.

1.4 Objetivos

1.4.1 General

Determinar la incidencia de la aplicación de las normas ISO 27001 y 27002 en la seguridad de las bases de datos de las Instituciones de Educación Superior.

1.4.2 Específicos

- Analizar la seguridad de las bases de datos en instituciones de Educación Superior.
- Realizar análisis de vulnerabilidad a bases de datos de una institución de Educación Superior.
- Determinar la aplicación de las normas ISO 27001 y 27002.
- Establecer una solución de seguridad en una institución de Educación Superior.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes Investigativos

Aguirre D, Palacios J, (2014), en la investigación denominada Evaluación técnica de seguridades del Data Center del Municipio de Quito según las normas ISO /IEC 27001:2005 SGSIE ISO/IEC 27002:2005., propone aplicar las normas ISO 27001:2005 y 27002:2005 para identificar vulnerabilidades de seguridad en todos los elementos del Data center y recomendar se establezcan políticas de seguridad de la información y controles para el manejo de riesgos, concluyendo la necesidad de una adecuada aplicación de políticas de seguridad y sus respectivas actualización, así como un plan de respaldo de información.

Mantilla A y Naranjo J, (2009), en la investigación denominada “Diseño de un sistema de gestión de seguridad de la información para cooperativas de ahorro y crédito en base a la norma ISO 27001”, plantea la necesidad de contar con un sistema de gestión de seguridad de la información para cooperativas de ahorro y crédito, considerando la importancia de la información financiera que manejan estas entidades; y en donde concluye, que el sistema de gestión de seguridad de la información debe ser revisado y actualizado de forma permanente para la máxima utilidad a la empresa.

Lache, (2015), en la investigación denominada “Diseño de un sistema de seguridad de la información para la compañía ACOTECNIC Cía. Ltda. basado en la norma NTE INEN ISO /IEC 27002”, realiza un estudio sobre necesidad de protección de la información mediante políticas de seguridad, una cultura de ética y un correcto modelo administrativo basado en objetivos claros y legislación

vigente que proteja los intereses de la empresa, concluyendo la necesidad de implementación de políticas de seguridad para la información.

2.1.1 Estado del Arte

El análisis respecto a la incidencia de la aplicación de normas ISO en instituciones de Educación Superior, se realizó en base a la revisión de implementaciones efectuadas y la investigación de resultados en diferentes Instituciones de Educación Superior, así:

La Universidad de Colima - México se encuentra certificada bajo la norma ISO 27001:2005 de Seguridad de la Información con 14 procesos administrativos, para lo cual ha establecido 8 políticas de seguridad de la Información, que conforme los dominios que establece la norma se enmarcan dentro de los siguientes:

Tabla 1 Dominios ISO 27001:2005. Universidad Colima - México

No	Dominio de seguridad de la norma ISO 27001:2005 relacionado	Política implementada
1	A.5 Política de seguridad de la información A.6 Aspectos organizacionales para la seguridad A.7 Gestión de activos A.11 Control de Acceso A.9 Seguridad física y ambiental A.10 Gestión de comunicaciones y operaciones	Política de buenas prácticas de usuario (La información y los activos de información)
2	A.9 Seguridad física y ambiental	Política de buenas prácticas en sites (preservar la C,I,A de los equipos y servidores)
3	A.10 Gestión de comunicaciones y operaciones A.15 Cumplimiento	Política de digitalización (preservar la C,I,A de la información digitalizada) Política de respaldo de información (preservar la C,I,A en medios electrónicos) Política para el control de archivos físicos (preservar la C,I,A de la información impresa)
4	A.10 Gestión de comunicaciones y operaciones A.12 Adquisición, desarrollo y mantenimiento de sistemas de información	Política de desarrollo de software (regular el desarrollo y mantenimiento de los sistemas informáticos)

No	Dominio de seguridad de la norma ISO 27001:2005 relacionado	Política implementada
	A.14 Gestión de la continuidad del negocio	
5	A.13 Gestión de incidentes de seguridad	Política de gestión de incidentes de seguridad (reporte, análisis, solución y aprendizaje de incidentes de seguridad)
6	A.8 Seguridad en recursos humanos	Política para el control y salida de empleados (asegurar la C,I,A por parte del personal)

Fuente: Sitio Oficial Universidad de Colima – México
Elaborado por: La Investigadora

La Universidad de Colima - México cuenta con un Comité del Sistema de Gestión Integral encargado de la implementación, monitoreo y evaluación del cumplimiento de la norma; coligiéndose la importancia que se da a la información en los sistemas institucionales.

Baldeón, M. y Guanopatín, J. (2015) en la investigación denominada *"Políticas de seguridad de la información para la Universidad Central del Ecuador bajo los estándares ISO/IEC 27000 y COBIT 5"* enmarcan su estudio aplicando la versión 2005 de las normas ISO y sus 11 categorías de control, que permite determinar el estado de madurez de los dominios de seguridad de la información. Allí se determina que los dominios con un nivel de cumplimiento entre el 15% y 50% tienen un nivel insuficiente de madurez y aquellos que están entre el 50% y el 85% han alcanzado un nivel suficiente de madurez. Luego del análisis de cada uno de los dominios se establecen los siguientes resultados:

Tabla 2 Nivel de madurez 27001: 2005 - U. Central del Ecuador

Categoría	Madurez	Vulnerabilidad
A5. Políticas de Seguridad de la Información	42,361% Insuficiente	Falta de políticas para la seguridad de la información
A.6 Aspectos Organizacionales para la Seguridad de la Información	36,111% Insuficiente	Área en reestructuración, no ha desarrollado e implementado políticas de seguridad
A.7 Gestión de Activos	49,296% Insuficiente	No cuenta con políticas para asegurar los activos de información
A.8 Seguridad de Recursos Humanos	49,653% Insuficiente	Falta definir y documentar los roles y responsabilidades de seguridad para empleados y proveedores
A.9 Seguridad Física y Ambiental	50,694% Suficiente	Falta de políticas que regulen las acciones del personal
A.10 Gestión de Comunicaciones y Operaciones	53,373% Suficiente	Es necesario se desarrollen e implementen políticas para todos los procesos de comunicaciones y operaciones
A11. Control de Acceso	62,847% Suficiente	Requiere desarrollo de políticas
A12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	64,063% Suficiente	Requiere desarrollo de políticas
A13. Gestión de Incidentes de Seguridad de la Información	39,789% Insuficiente	No se cuenta con una bitácora de incidentes ni una política para administrar los eventos de seguridad.
A.14 Gestión de la Continuidad del Negocio	44,097% Insuficiente	No posee un plan integral para la continuidad del negocio. Existen directrices para ciertos procesos críticos.
A.15 Cumplimiento	37,676% Insuficiente	Falta de reglamentos que regulen o eviten las violaciones de los requerimientos de seguridad

Fuente: Baldeón, M. y Guanopatín, J. (2015)
Elaborado por: La Investigadora

Finalmente se concluye sobre la importancia de implementar políticas de seguridad a fin de poder preservar y administrar la información.

Tixilima, V (2015), en la investigación denominada "*Elaboración de políticas y normas de seguridad de la información en base a la norma de seguridad ISO/IEC 27001, y al análisis de riesgos realizado aplicando la metodología Magerit y la herramienta Pilar. Caso de estudio: Universidad Politécnica Salesiana Sede Quito Campus Sur*", utiliza la revisión 2013 de la norma, la metodología Magerit y el software Pilar para identificar y valorar los activos, asignando una mayor

ponderación entre los activos al portal web, sistema de nivelación y las comunicaciones de red, sobre los cuales se obtiene el informe de amenazas que puedan afectar a la confidencialidad, integridad, disponibilidad y autenticación de usuarios, y propone el modelo de políticas de seguridad de la información.

Torres, H (2010), en la investigación titulada: "*Diseño de la seguridad informática en la implementación del Data Center de la Universidad Nacional de Loja",* realiza tres fases importantes, una de diagnóstico de la situación actual, el desarrollo de la solución y el manual de políticas; en la primera se identifica las condiciones actuales de la infraestructura hardware y la red de comunicaciones; en la segunda se plantean soluciones concretas respecto a la configuración de la red para prevenir la materialización de los riesgos de seguridad y en la tercera se plantea un manual de políticas de seguridad informática basado en la norma ISO/IEC 27000. Finalmente se concluye la necesidad de actualización de la infraestructura física y lógica, la falta de capacitación del recurso humano y la necesidad de implementar políticas de seguridad de la información.

Para analizar el estado actual respecto a la Universidad Nacional de Chimborazo, se implementó una Auditoría con base a los 14 objetivos y 114 controles de seguridad que establecen las normas 27001 y 27002.
Parte de dicha auditoría constituyó el análisis de vulnerabilidades de las bases de datos que contienen la información del sistema académico, para determinar posibles riesgos a los que pueda estar expuesta la información. (ver anexos).

2.2. Fundamentación Filosófica

La presente investigación se enmarca en el paradigma crítico propositivo, es crítico porque realiza un análisis crítico del problema, y es propositivo porque busca proponer una solución factible al problema.

2.3. Fundamentación Legal

La Ley Orgánica de Transparencia y Acceso a la Información Pública en su Artículo 10 sobre la custodia de la información, habla de la responsabilidad de las instituciones públicas y personas jurídicas de derecho público sobre el manejo profesional de la información sin justificación de ausencia de normas técnicas que obstaculice el acceso a información pública.

El Acuerdo Ministerial No. 166, publicando en el Registro Oficial 88 del 25 de septiembre de 2013, dispone a las entidades de la Administración Pública Central y dependientes de la función Ejecutiva la implementación del esquema gubernamental de seguridad de la información EGSI, Norma Técnica Ecuatoriana INEN ISO/IEC 27002 “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”, para garantizar la seguridad y confianza como parte del Plan Estratégico de Seguridad y Protección de Datos.

Las Normas ISO 27001 y 27002 son estándares internacionales legalmente reconocidos y aplicados al ámbito nacional mediante las Normas INEN NTE INEN-ISO/IEC 27001 y 27002.

Las normas de control interno de la Contraloría General del Estado, dentro del grupo 400 Actividades de Control, determina la necesidad de establecer políticas y procedimientos para proteger y conservar los activos, así como el acceso a los sistemas de información.
El subgrupo 410 Tecnología de la Información con las normas desde las 01 hasta la 17 establece las directrices que deben tomar en cuenta las entidades del sector público respecto a todos los procesos de acceso a la información como separación de funciones, plan estratégico, políticas, administración de proyectos, desarrollo y adquisición de software, adquisición y mantenimiento de infraestructura, seguridad, soporte técnico, monitoreo y capacitación entre otros. (Contraloría General del Estado. 2009, pg. 9, 68-75).

En el Reglamento del Centro de Cómputo de la UNACH en el Art 5. Son obligaciones y atribuciones del Director, literal b) dice: “Organizar, distribuir y administrar eficaz y eficientemente los recursos bajo custodia del personal del Centro, de manera que satisfaga las necesidades de las diferentes facultades, carreras y usuarios en general”.

El literal d) indica “Gestionar la adquisición de hardware y software requerido para el desarrollo de las actividades del Centro de Cómputo”.

En el artículo 7 dentro de las funciones de los asistentes técnicos en el literal c) dice: “Aplicar buenas prácticas de seguridad”

En la Constitución Política del Ecuador, la Ley Orgánica de Educación Superior y el Estatuto de la UNACH, no existe ninguna regulación o impedimento relacionado a la aplicación de normas de seguridad, por lo que no existe restricción legal para el desarrollo de la presente investigación.

2.4. Categorías fundamentales

Las normas ISO 27001 y 27002 y su incidencia en la seguridad de la información

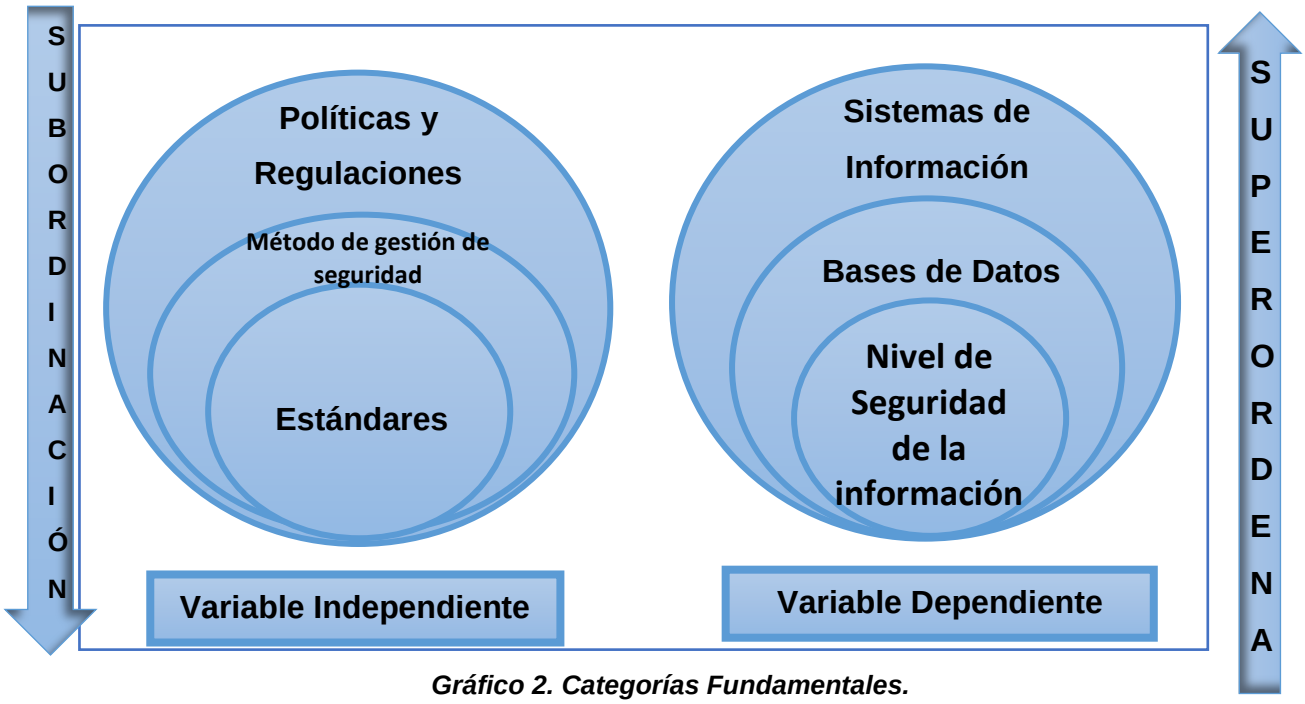


Gráfico 2. Categorías Fundamentales.
Elaborado por: La Investigadora

2.4.1 Categorías Fundamentales de la Variable Dependiente

La Información

Para Gilles Deleuze (1990), la información es un sistema de control, en tanto que es la propagación de consignas que deberíamos de creer o hacer que creemos.

Según el Diccionario de la Real Academia de la Lengua Española, la definición 5 de información es catalogada como: Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.

Bases de Datos

“Una definición de base de datos dice que es la colección de datos organizada para dar servicio eficientemente a muchas aplicaciones al centralizar los datos y minimizar aquellos que son redundantes”. (Laudon, 2010).

Es un conjunto de datos que generalmente describe las actividades de una o varias organizaciones relacionadas. (Ramakrishnan, 2010, pg. 4).

Sistema de Gestión de Bases de Datos

Un sistema de gestión de bases de datos consiste en una colección de datos interrelacionados y los programas que permiten acceder a ellos. (Silberschatz, 2006, pg. 1).

Niveles de Abstracción

Según Ramakrishnan (2010) los datos en el SGBS se describen en tres niveles de abstracción: conceptual, físico y externo:

- El esquema físico, nivel más bajo de abstracción, define como se almacenarán los datos y su forma de acceso que se construye en el diseño físico de la base de datos.
- El esquema conceptual, también denominado como lógico, se define mediante el lenguaje de definición de datos (DDL) y describe los datos almacenados y sus relaciones.
- El esquema externo o de vistas permite personalizar el acceso a los datos conforme los permisos y necesidades de los usuarios; también se define mediante el DDL.

Ventajas de los Sistemas de Gestión de Base de Datos

Para Ramakrishnan (2010) son:

- Independencia con respecto a los datos.
- Acceso eficiente a los datos.
- Integridad y seguridad de los datos.
- Administración de los datos.
- Acceso concurrente y recuperación en caso de fallo.
- Reducción del tiempo de desarrollo de las aplicaciones.

Sistemas de Información

Conforme la Ley de Comercio Electrónico, firmas y mensajes de datos un Sistema de Información “es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos”. (Ley de Comercio Electrónico, pg. 15)

Un sistema de información es un conjunto de componentes que recolectan, procesan, almacenan y distribuyen información para la toma de decisiones. (Laudon, 2010).

Los sistemas de información requieren ser interoperables y poseer una infraestructura tecnológica robusta que garantice su accesibilidad y disponibilidad permanente.

Estos ejecutan tres actividades fundamentales: la captura (recolección de datos), procesamiento (transformación de datos) y salida (reportes) de información, utilizando de forma paralela también la retroalimentación que permita validar la etapa de alimentación (Laudon, 2010).

Seguridad de la Información

Seguridad Informática es “cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios de usuarios autorizados al sistema). (Gómez, 2011, p. 38).

Objetivos

Para Gómez (2011) son:

- Minimizar los riesgos detectando amenazas y problemas.
- Limitar las pérdidas y garantizar la disponibilidad del sistema, en caso de incidentes de seguridad.
- Garantizar la utilización de los recursos y aplicaciones del sistema.
- Cumplir con el marco legal y los requisitos de funcionamiento establecidos.

Estos objetivos se pueden alcanzar con acciones encaminadas a fortalecer el plano humano, técnico de organización y legislación, como muestra la Gráfico No. 3.

Gráfico 3 Planes de actualización a la seguridad informática
Fuente: Enciclopedia de la seguridad informática (Gómez, 2011, p. 41)
Elaborado por: La Investigadora

Servicios de seguridad de la información

Según Gómez (2011) son:

- **Confidencialidad. –** Garantía de que la información podrá ser leída únicamente por las personas interesada.
- **Autenticación. -** Garantía de la identidad del creador de un mensaje o de quien accede a un equipo, red o servicio.
- **Integridad. -** Garantía de que la información no ha sido modificada en el proceso de transmisión.
- **No repudio. -** Mecanismo probatorio para demostrar la autoría y envío y recepción de un mensaje.

- **Disponibilidad. –** Garantizar el correcto funcionamiento, incluso frente a ataques o interferencias.
- **Autorización. –** Capacidad de acceso a los recursos, conforme los permisos otorgados.
- **Auditabilidad. –** Monitoreo de la utilización de los recursos del sistema para detectar comportamiento anómalo, rendimiento y volumen de transacciones.
- **Reclamación de origen. –** Permite probar quien ha sido el creador de un mensaje o documento.
- **Reclamación de propiedad. –** Permite probar quien posee los derechos de autor de alguna información.
- **Anonimato en el uso de los servicios. –** Garantizar el acceso confidencial a ciertos servicios.
- **Protección a la réplica. –** A fin de evitar ataques de repetición que generen operaciones no deseadas en el sistema.
- **Confirmación. –** Que permita confirmar la realización de una operación
- **Referencia temporal. –** Permite demostrar el instante en que se efectuó una operación.
- **Certificación mediante terceros de confianza. –** Organismos que se encargan de certificar la realización y contenido de las operaciones y avalar sus intervinientes.

Control Interno Informático

Cualquier actividad realizada para prevenir o corregir errores o irregularidades que puedan afectar el funcionamiento de un sistema. Siendo estos: preventivos, detectivos y correctivos. (Piattini, 2008, pg. 9).

Para Piattini (2008), el sistema de control deberá definirse sobre tres aspectos fundamentales que son:

- Gestión de los sistemas: políticas, normas, directrices y controles que sirvan para diseñar e implantar los sistemas.
- Administración de los sistemas: Los controles respecto a la operación y transmisión de datos.
- Seguridad: Sobre la confidencialidad de los datos (control de acceso, integridad (correctos y completos) y disponibilidad (permanencia en tiempo).

Niveles de madurez en la gestión de seguridad

Según Gómez (2011), son cuatro niveles de madurez, así:
Etapa 1: Es la implantación de medidas básica o por sentido común que se establecen en cualquier sistema, lo cual llega en algún momento a resultar insuficiente para garantizar la gestión de riesgos.
Etapa 2: Es la adaptación a requisitos legales, normativas, protección de datos personales y propiedad intelectual, etc.
Etapa 3: Es la definición de políticas, procedimientos, análisis y gestión de riesgos, así como un plan de atención de incidentes y de continuidad del negocio.
Etapa 4: Se refiere a la certificación bajo un estándar de buenas prácticas en seguridad.

Auditoría Informática

Según Mario Piattini la Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema salvaguarda los activos, mantiene la integridad de sus datos y utiliza eficientemente los recursos. (Piattini, 2008, pg. 7).

Es la revisión y evaluación de controles, sistemas y procedimientos informáticos; su uso, eficiencia y seguridad, que permita una utilización, más eficiente, confiable y segura de la información. (Echenique, 2001, pg. 18).

Fases de la auditoría informática

Para Echenique (2011), las fases son:

- Planeación. - Determinar el tamaño y características del área a auditar, así como el alcance de la misma, considerando: evaluación administrativa del área, de los sistemas y procedimientos, de los equipos, del proceso de datos, seguridad y confidencialidad y aspectos legales.
- Revisión preliminar. – Recolección de evidencias por medio de entrevistas, observación y revisión documental. Permite elaborar el plan de trabajo.
- Revisión detallada. –Permite tener un conocimiento amplio de los controles usados en el área informática. Permite realizar una evaluación del riesgo.
- Evaluación de la información. – Con la información, suficiente, relevante y útil, e incluyendo el empleo de pruebas selectivas y muestreo, se deberá interpretar y documentar la información con objetividad respecto a los hallazgos determinados.
- Pruebas de conocimiento. – Evaluación de la efectividad de los controles implementados.
- Pruebas de control de usuario. – Perspectiva desde el punto de vista del usuario mediante entrevistas, encuestas o evaluaciones hechas con los usuarios.
- Pruebas sustantivas. – Determinar cuándo pueden ocurrir pérdidas materiales durante el procesamiento de la información.
- Interpretación de la información. – Manejo de técnicas que permita realizar un análisis crítico respecto a los hechos auditados, la madurez del sistema y los puntos vulnerables.
- Conclusiones. – presenta una breve descripción del momento actual, problemas, fallos y repercusiones. De forma alternativa se puede plantear soluciones.

2.4.2 Categorías Fundamentales de la Variable Independiente

Políticas y procedimientos de seguridad

La constitución del Ecuador en su artículo 66, numeral 19 reconoce: “El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley”. (Asamblea Constituyente, sf, pg. 49).

El artículo 92 de la constitución dice: “Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Así mismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.
La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados”. (Asamblea Constituyente, sf, pg. 66).

El literal d) del artículo 2 de la Ley Orgánica de Transparencia y Acceso a la Información Pública garantiza la protección de la información personal en poder del sector público y/o privado.

En la Ley del Sistema Nacional de Registro de Datos Públicos su artículo 4 dice: "Responsabilidad de la información. - Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información.
Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal.
La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución".

El artículo 6 de la mencionada ley dice: "Accesibilidad y confidencialidad. -
Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.
El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial.
También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado.

La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos.
Para acceder a la información sobre el patrimonio de las personas el solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará de la misma y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer.
La Directora o Director Nacional de Registro de Datos Públicos, definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad".

La Ley de Comercio Electrónico, firmas y mensajes de datos en su disposición general novena sobre el glosario de términos define a la Intimidad como: "El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados". (Ley de Comercio Electrónico, pg. 16).

Métodos de gestión de seguridad

Entendido el método como el procedimiento que se sigue en las ciencias para hallar la verdad y enseñarla. (Real Academia de la Lengua Española, definición 4); la gestión de seguridad de la información se puede direccionar así:

- De manera empírica, con base a la experiencia u observación.

- Basada en el cumplimiento de estándares, como la aplicación de las normas ISO 27000.

Familia ISO /IEC 27000

Son un conjunto de estándares para gestionar la Seguridad de la Información, cuyos objetivos son:

- Identificar y ordenar las normas de seguridad de la información
- Normar las directrices de seguridad.
- Establecer los requisitos, metodologías y técnicas de valoración, armonizando entre las diferentes normas.
- Emplear un lenguaje común
- Flexibilidad para la selección e implantación de controles. (Gomez, A. 2011. Pg. 159)

Norma ISO 27001

ISO 27001: Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información - Requisitos es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (ISO, 2015).

Norma ISO 27002

ISO 27002: Tecnologías de la información – Técnicas de Seguridad – Código de Práctica para los controles de seguridad de la información es un catálogo de buenas prácticas que determina, desde la experiencia, una serie de objetivos de

control, y controles que se integran dentro de todos los requisitos de la norma ISO 27001 en relación con el tratamiento de los riesgos. (ISO, 2015).

Normas NTE INEN-ISO/IEC 27001 y 27002

Estas normas ecuatorianas son una traducción idéntica de las normas Internacional ISO/IEC 27001 y 27002, las cuales serán utilizadas para la presente investigación. (INEN, 2017).

Estructura de la Norma NTE INEN-ISO/IEC 27001

En ISO/IEC, 2015 - INEN, 2017, podemos ver que los tres primeros capítulos se orientan a una explicación general respecto a la norma y su aplicación, los demás capítulos son los requisitos exigidos para su implementación, así:

1. Objeto y campo de aplicación: Orientación, uso y finalidad del estándar.
2. Referencias normativas: Recomendación de consulta de ciertos documentos.
3. Términos y definiciones: Terminología aplicable al estándar.
4. Contexto de la organización: Contiene las indicaciones sobre el conocimiento de la organización, sus necesidades y expectativas para el sistema de gestión de seguridad de la información
5. Liderazgo: Compromiso de la alta gerencia para elaborar una política de seguridad que sea socializada y contenga roles, responsabilidades y autoridades.
6. Planificación: Determinar riesgos, y oportunidades y establecer objetivos de seguridad de la información.
7. Soporte: Contar con los recursos, competencias, conciencia e información documentada para cada caso.
8. Operación: Planificar, implementar y controlar los procesos de la organización, valorar y tratar los riesgos.

9. Evaluación del desempeño: Seguimiento, medición, evaluación, auditoría interna para verificar el adecuado funcionamiento.
10. Mejora: Importancia de mejora continua, resolución de no conformidades.

Estructura de la Norma NTE INEN-ISO/IEC 27002

Según ISO/IEC, 2015 - INEN, 2017, contiene 14 capítulos de controles de seguridad con un total de 35 categorías y 114 controles, siendo los objetivos de control:

1. A5. Política de seguridad de información
2. A6. Organización de seguridad de la información
3. A7. Seguridad en recursos humanos
4. A8. Gestión de activos
5. A9. Control de acceso
6. A10. Criptografía
7. A11. Seguridad física y del entorno
8. A12. Seguridad de las operaciones
9. A13. Seguridad en las comunicaciones
10. A14. Adquisición, desarrollo y mantenimiento del sistema
11. A15. Relaciones con proveedores
12. A16. Gestión de incidentes de seguridad de la información
13. A17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio.
14. A18. Cumplimiento

Con los conceptos previamente revisados y considerado que el valor que poseen las bases de datos son los datos que contienen y la información que se procesa de las mismas, en adelante, la terminología de seguridad de las bases de datos estará inmersa en las aseveraciones respecto a seguridad de la información.

2.5. Hipótesis

Las normas ISO 27001 y 27002 SI inciden en la seguridad de la información

2.6. Señalamiento de Variables

Variable Independiente: Las normas ISO 27001 y 27002

Variable Dependiente: Seguridad de la Información

CAPÍTULO III

METODOLOGÍA

3.1 Enfoque

La investigación tiene un enfoque cuali – cuantitativo.

Cuantitativa porque utilizó parámetros de medición para determinar la seguridad de la información en las bases de datos institucionales.

Cualitativa porque se emiten juicios de valor sobre la eficiencia en la seguridad en la información de las bases de datos.

3.2 Modalidad Básica de Investigación

Las modalidades de investigación son Bibliográfica y de Campo.

Investigación Bibliográfica

Porque utiliza fuentes como libros, documentos, artículos, revistas, etc., para la construcción del marco teórico y el análisis de la aplicación de las normas ISO en diferentes instituciones de Educación Superior.

Investigación de Campo

Porque busca aplicar una auditoría de seguridad de la información en las bases de datos mediante la aplicación de las normas ISO 27001 y 27002.

Investigación Documental

Por cuanto se analiza los resultados de la auditoría para proponer una solución a la institución.

3.3 Nivel o tipo de investigación

La investigación es:

- **Experimental –** al realizar el análisis sobre la seguridad de la información en las bases de datos. Si no existen las condiciones propicias, realizar una propuesta que solucione el problema.

- **Descriptiva –** porque con el análisis se determinará las deficiencias en la seguridad de las bases datos.

- **Explicativa –** Para determinar en base al análisis anterior si existe la necesidad de mejorar la seguridad de las bases de datos.

- **Correlacional –** Porque busca medir el grado de relación existente entre las normas ISO 27001 y 27002 y la seguridad de las bases de datos.

3.4 Población y Muestra

La población para la presente investigación está constituida así:

Tabla 3. Población y Muestra

No	Tipo de Población	Descripción	Número
1	Personal de la Unidad Técnica de Control Académico	Coordinador Administrador de Bases de Datos Desarrollador de Sistemas	3
2	Administración de la red institucional	Administrador de la red institucional	1
3	Operadores del sistema académico	Personal de secretaría que utiliza el sistema académico	51
4	Estudiantes	Estudiantes registrados con usuario para el acceso web al sistema académico	10.063
5	Docentes	Docentes registrados con usuario para el acceso web al sistema académico	548
TOTAL			**10.666**

Elaborado por: La Investigadora

Para el caso de la población del Personal de la Unidad Técnica de Control Académico, Administración de la red institucional y Operadores del sistema académico se trabajó con la población total considerando que es un grupo pequeño.

Para el cálculo de la muestra de estudiantes y docentes se utilizó la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Donde:

n = tamaño de la muestra

N = población

Z = nivel de confianza 95% equivalente a 1,96

σ = Desviación estándar constante 0,5

e = margen de error: 10%

El tamaño de la muestra de estudiantes es de: 95

El tamaño de la muestra de docentes es de: 82

Para la selección de la muestra de docentes y estudiantes se utilizó el método probabilístico aleatorio simple, es decir escogiendo de forma aleatoria tantos usuarios como requiera completar la muestra.

3.5 Operacionalización de las variables

Variable Independiente: Normas ISO 27001 y 27002

Tabla 4. Operacionalización de la Variable Independiente

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS
La norma ISO 27001 permite gestionar la seguridad de la información.	Objetivos	Nivel de madurez del objetivo de control	¿Se cuenta con políticas de seguridad de la información?	Encuesta: Cuestionario Entrevista: Guía de la Entrevista
La norma ISO 27002 complemento de la anterior es un catálogo de buenas prácticas para la seguridad de la información.	Controles	Nivel de madurez del control	¿Se encuentran identificados los activos de información?	Observación: Análisis Documental

Elaborado por: Investigadora

Variable Dependiente: Nivel de Seguridad de la Información

Tabla 5. Operacionalización de la Variable Dependiente

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS
Medidas preventivas y correctivas orientadas a mantener la confidencialidad, integridad y disponibilidad de la misma	Inexistente Etapa 1 de madurez Etapa 2 de madurez Etapa 3 de madurez	Disponibilidad Integridad Confiabilidad	¿Se maneja algún estándar para la seguridad de la información? ¿Están identificados los riesgos respecto a los activos de información? ¿La información de los SGBD cumple con las características de disponibilidad, confiabilidad e integridad?	Encuesta: Cuestionario Entrevista: Guía de la Entrevista Observación: Análisis Documental Análisis de vulnerabilidades

Elaborado por: La Investigadora

3.6 Plan de recolección de información

Para el análisis de la aplicación de las Normas ISO 27001 y 27002, así como su incidencia en la seguridad de las bases de datos en instituciones de educación superior, se realizó una investigación documental con base a propuestas de implementación de dichas normas.

Para el análisis de la aplicación de las normas en la Universidad Nacional de Chimborazo, se realizó un plan de auditoría sobre el nivel de madurez de cada uno de los objetivos y controles de seguridad que establece la norma, sustentado además en la aplicación de encuestas, entrevistas, análisis de vulnerabilidades y el respaldo documental de información institucional.

3.7 Plan de Procesamiento y análisis de la Información

Para el procesamiento y análisis de la información se aplicó los siguientes procedimientos:

Procesamiento de la Información

1. Elaboración de instrumentos para entrevista y encuestas.
2. Elaboración de matriz de evaluación del nivel de madurez de los controles de seguridad conforme normas 27001 y 27002.
3. Tabulación de la información obtenida
4. Estudio estadístico de datos para presentación de resultados.

Análisis de resultados

1. Análisis crítico de la información recolectada.
2. Análisis de los resultados estadísticos, relación con los objetivos e hipótesis.
3. Interpretación de los resultados.
4. Comprobación de hipótesis para la verificación.
5. Establecimiento de conclusiones y recomendaciones.

CAPÍTULO IV

ANÀLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis e interpretación de resultados

Para el análisis e interpretación de resultados se consideran tres momentos respecto al proceso de investigación sobre la seguridad de la información, así:

1. Encuestas a usuario. – Para analizar desde la visión del usuario su percepción, conocimiento y comprometimiento respecto a la seguridad de la información a la que accede. Complementario al proceso de investigación.

2. Resultados auditoría seguridad de la información. – Que permita determinar el nivel de madurez respecto a los controles de seguridad que establece la norma. Se utiliza para verificar la hipótesis.

3. Análisis de la incidencia de la aplicación de las normas ISO en la seguridad de las bases de datos de las Instituciones de Educación Superior. – Que permita comparar los resultados de estudios en otras Instituciones de Educación Superior con los resultados de la UNACH y emitir un juicio de valor respecto a la necesidad de seguridad de la información en las IES.

- Respecto al punto 1, la aplicación de encuestas a los usuarios (estudiantes y docentes) y operadores del sistema académico (personal de secretaría), se realizó con la finalidad de complementar la información respecto a las políticas de seguridad, para poder establecer un juicio de valor referente al conocimiento y responsabilidad con que se manipula la información del sistema, obteniéndose los siguientes resultados, por objetivo de control:

1. **¿Cuenta la institución con alguna política de seguridad de la información para los sistemas a los que accede?**

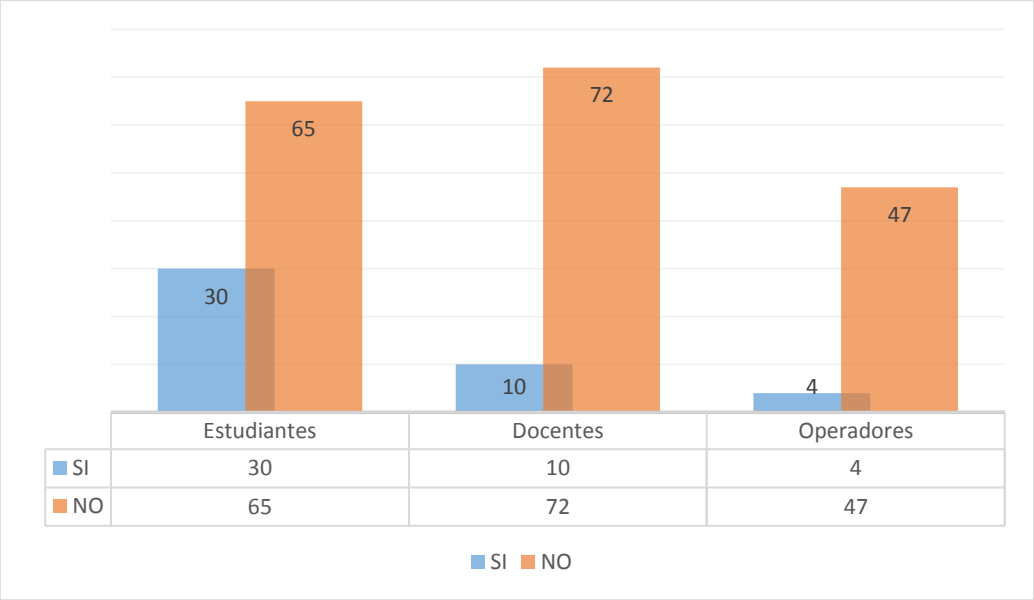


Gráfico 4 Pregunta respecto al Objetivo de Control A5. Política de seguridad de la información
Elaborado por: La Investigadora

Análisis: 184 encuestados equivalente al 80,70% indica que la institución no cuenta con una política de seguridad de la información para los sistemas a los que accede, mientras 44 encuestados equivalente que un 19,30% manifiesta que la institución si cuenta con alguna política de seguridad.

Interpretación: Los resultados obtenidos permiten concluir que el 80,70% de usuarios y operadores desconocen si la institución ha implementado alguna política de seguridad respecto a la información, por lo tanto, de haber alguna, esta no ha sido socializada y no se ha capacitado a los usuarios al respecto.

2. **¿Se encuentra su equipo de cómputo protegido y actualizado contra malware?**

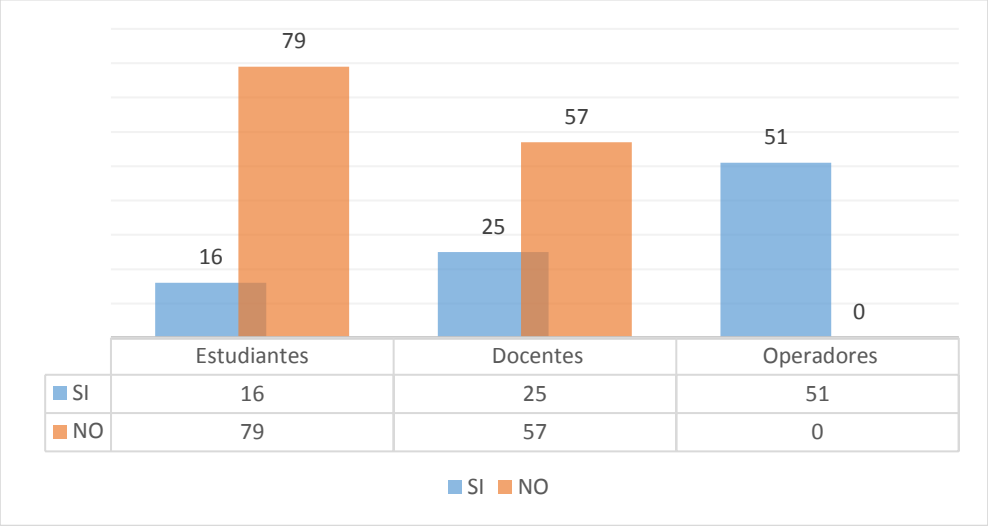


Gráfico 5 Pregunta respecto al Objetivo de Control A6. Organización de seguridad de la información
Elaborado por: *La Investigadora*

Análisis: 136 encuestados equivalente al 59,65% manifiesta no tener su equipo protegido y actualizado contra malware, 92 encuestados equivalente al 40,35% manifiesta si tener su equipo protegido contra malware.

Interpretación: Más del 50% de los encuestados reconoce que sus equipos de cómputo no se encuentran protegidos o actualizados contra malware, lo cual representa un riesgo a la seguridad de la información, considerando que son susceptibles a la ejecución de programas maliciosos que pueden aprovechar alguna vulnerabilidad para intentar acceder a datos sensibles de la institución.

3. ¿Ha recibido capacitación para el manejo del sistema?

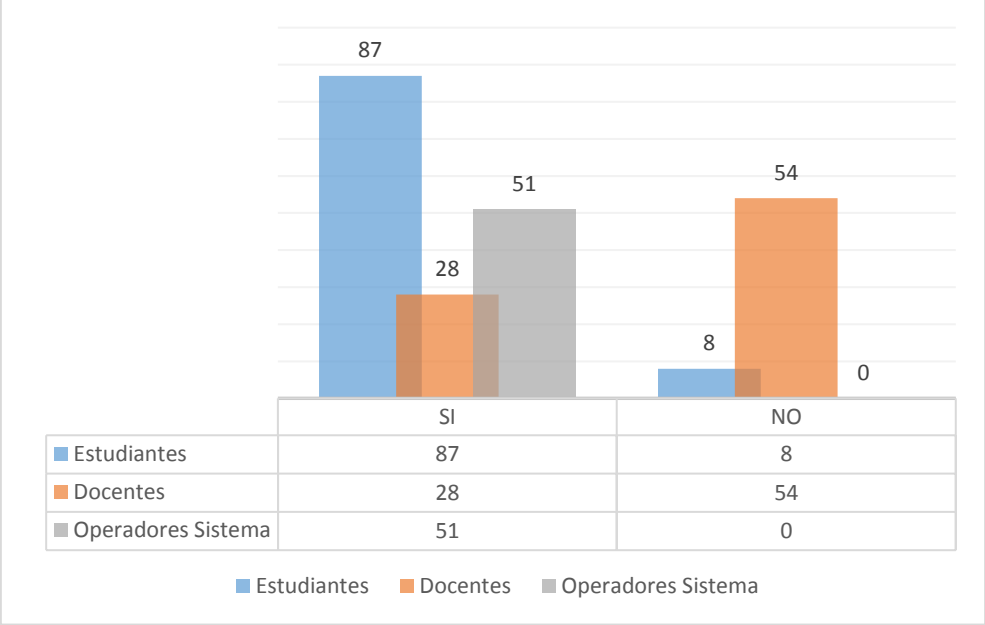


Gráfico 6 Pregunta respecto al Objetivo de Control A7. Seguridad en recursos humanos
Elaborado por: La Investigadora

Análisis: 166 encuestados equivalente al 72,81% manifiesta si haber recibido capacitación para el manejo de los sistemas, 62 encuestados equivalente al 27,19% indica no haber recibido la referida capacitación.

Interpretación: Al menos un 72,81% de usuarios reconoce haber recibido capacitación para el uso de los sistemas a los que accede. Se puede observar que el porcentaje mayor se identifica en el personal docente, quienes en ocasiones no asisten a los eventos de capacitación programados. La capacitación es únicamente en el funcionamiento de la aplicación.

4. **¿Ha sido sancionado alguna vez por proporcionar información sin autorización, de los sistemas a los que tiene acceso?**

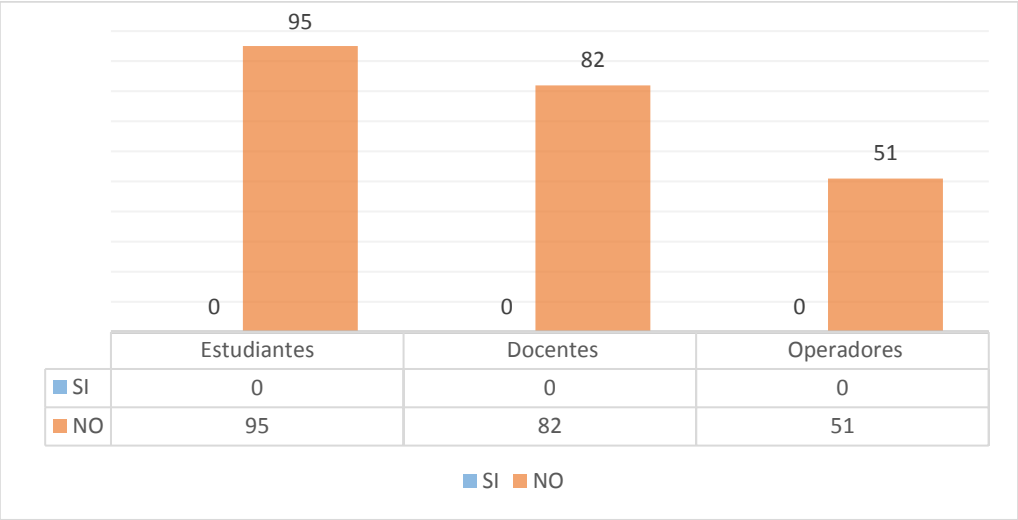


Gráfico 7 Pregunta respecto al Objetivo de Control A7. Seguridad en recursos humanos
Elaborado por: *La Investigadora*

Análisis: 228 encuestados equivalente al 100% manifiesta no haber sido sancionado por proporcionar información de los sistemas a los que accede.

Interpretación: Los encuestados indican no haber proporcionado información de los sistemas a los que acceden por cuanto tienen acceso únicamente a su información de interés (estudiantes), se utiliza para fines académicos (docentes) y solo se proporciona con autorización (operadores de sistema).

5. **¿Ha sido llamado la atención o sancionado alguna vez por manejo o uso inadecuado de claves de usuario?**

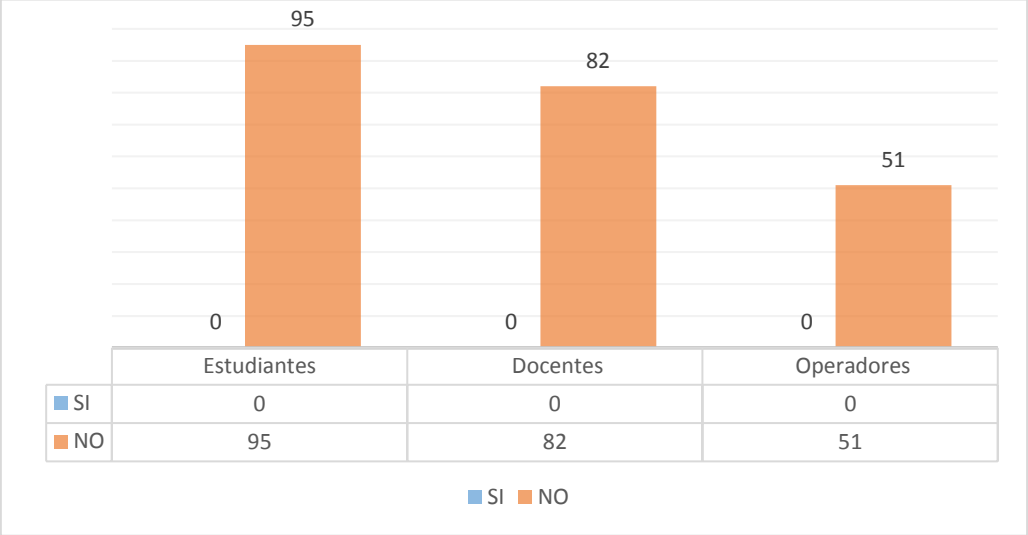


Gráfico 8 Pregunta respecto al Objetivo de Control A7. Seguridad en recursos humanos
Elaborado por: *La Investigadora*

Análisis: 228 encuestados equivalente al 100% manifiesta no haber sido llamado la atención o sancionado por manejo inadecuado de claves de usuario.

Interpretación: No han sido identificados incidentes de seguridad respecto al uso de credenciales de acceso por tanto hay usuarios sancionados; sin embargo, tampoco existe un procedimiento formal que establezca como actuar en estos casos.

6. **Si usted ha cambiado de función o salido a alguna otra área de trabajo en la institución. ¿Sabe si su usuario y privilegios de acceso anteriores fueron inhabilitados?**

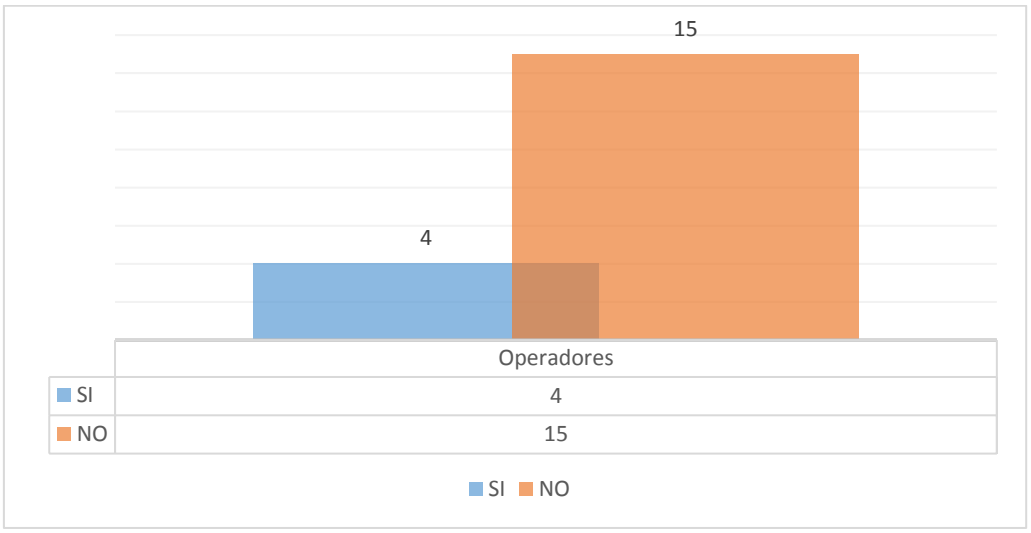


Gráfico 9 Pregunta respecto al Objetivo de Control A7. Seguridad en recursos humanos
Elaborado por: *La Investigadora*

Análisis: De los 51 encuestados, 19 equivalente al 37,25% manifiesta haber cambiado de área de trabajo; de los cuales 15 equivalente al 78,95% indica desconocer si sus privilegios de acceso anteriores fueron revocados; 4 equivalente al 21,05% indica si saber que sus privilegios anteriores fueron revocados.

Interpretación: Al existir un 78,95% de usuarios operadores del sistema que desconoce si sus privilegios de acceso fueron revocados, se puede evidenciar que no existe un procedimiento formalmente implantado respecto a los requisitos de seguridad para acceso a sistemas, por lo que, de no ser notificada la unidad encargada, los privilegios de ciertos usuarios podrían mantenerse por tiempo adicional al que por funciones a cargo tenga realmente derecho de acceso.

7. **De mantener aún acceso a sistemas de alguna función anterior. ¿Ha ingresado usted a dichos sistemas?**

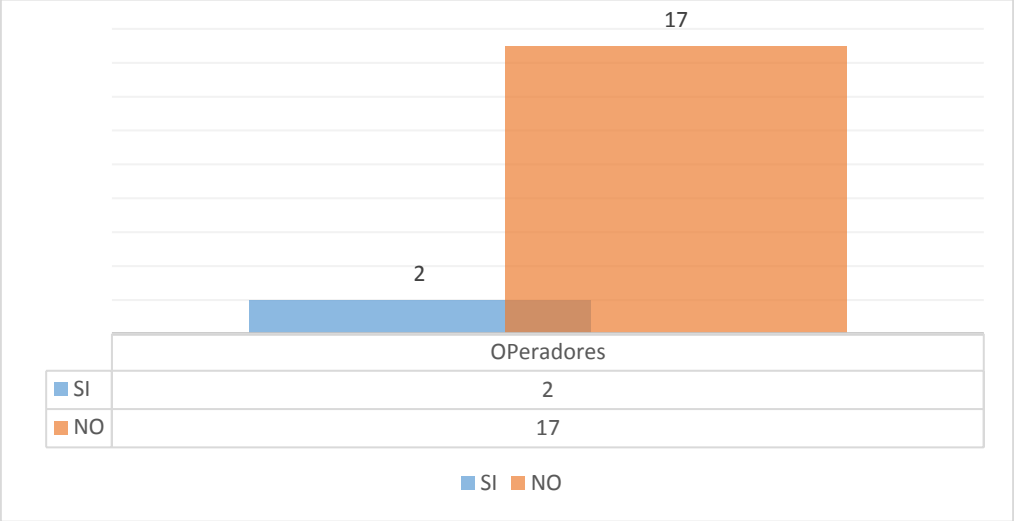


Gráfico 10 Pregunta respecto al Objetivo de Control A7. Seguridad en recursos humanos
Elaborado por: *La Investigadora*

Análisis: 2 encuestados equivalente al 10,53% manifiesta si haber ingresado al sistema cuando ya no cumplía una función relacionada, mientras el 89,47% indica no haberlo hecho.

Interpretación: A pesar de haberse identificado únicamente 2 casos de usuarios que reconocen haber ingresado al sistema cuando ya no cumplían una función asociada a ese privilegio, se puede evidenciar que el no contar con un procedimiento formal para revocar privilegios puede comprometer la seguridad de la información. Los encuestados manifiestan haber ingresado únicamente para consulta de información.

8. **¿Conoce usted si la institución tiene alguna política de protección de datos y divulgación de información**

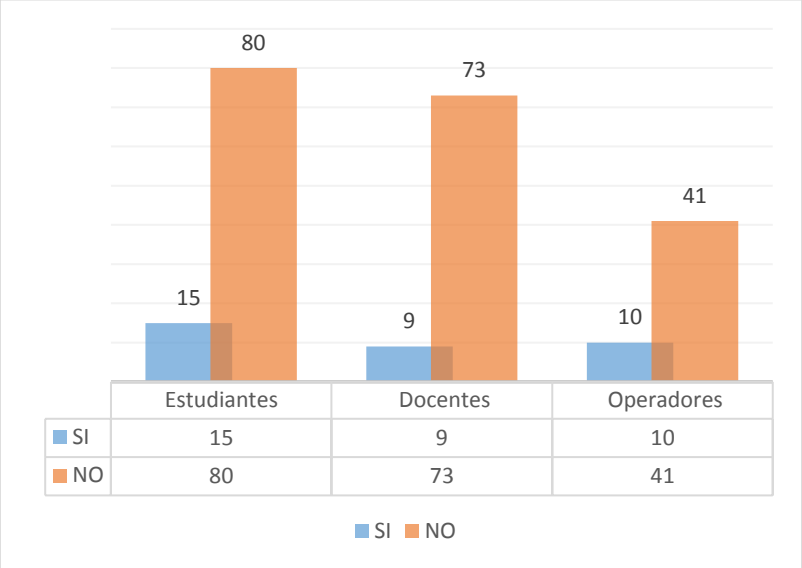


Gráfico 11 Pregunta respecto al Objetivo de Control A8. Gestión de activos
Elaborado por: La Investigadora

Análisis: 194 encuestados equivalente al 85,09% manifiesta desconocer si la institución tiene alguna política de protección de datos y divulgación de información; 34 encuestados equivalente al 14,91% indica si conocer que la institución maneje una política de protección de datos.

Interpretación: El 85,09% de usuarios desconoce que en la institución se maneje alguna política de protección de datos y divulgación de información, por lo qué, los datos como información personal, podrían ser divulgados por el desconocimiento de los usuarios respecto al uso de información.

9. **¿Conoce usted si alguna información a la que usted accede tiene restricción de divulgación?**

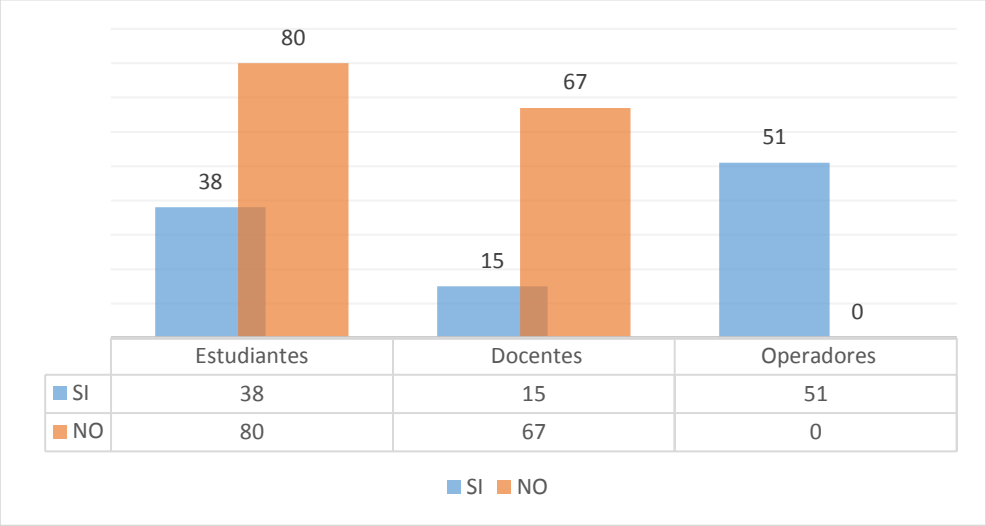


Gráfico 12 Pregunta respecto al Objetivo de Control A8. Gestión de activos
Elaborado por: La Investigadora

Análisis: 104 estudiantes equivalente al 41,43% manifiesta si conocer que la información a la accede tiene restricción de divulgación, mientras que el 58,57% desconoce si la información a la que accede tiene restricción de divulgación.

Interpretación: El 58,57% de los encuestados desconoce si la información a la que accede tiene restricción de divulgación por lo que información sensible podría ser expuesta por desconocimiento. El 100% de operadores encuestados puede entregar información, previo a un trámite aprobado, el cual no está necesariamente asociado a la protección de información, sino al cumplimiento de procedimientos implementados.

10. **¿Ha recibido alguna capacitación institucional sobre prácticas de seguridad de la información?**

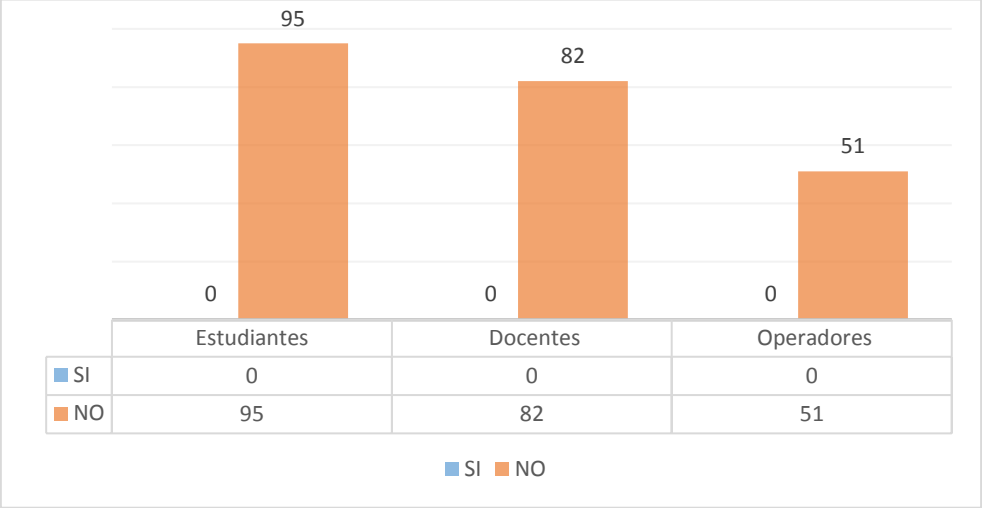


Gráfico 13 Pregunta respecto al Objetivo de Control A9. Control de acceso
Elaborado por: La Investigadora

Análisis: 228 encuestados equivalente al 100% manifiestan no haber recibido nunca una capacitación respecto a seguridad de la información.

Interpretación: Una vulnerabilidad respecto a la seguridad de la información, la representa precisamente el recurso humano, por lo que, su falta de capacitación en prácticas de seguridad podría representar una amenaza potencial respecto a la confidencialidad e integridad de la información.

11. ¿Ha experimentado dificultades de acceso al sistema académico?

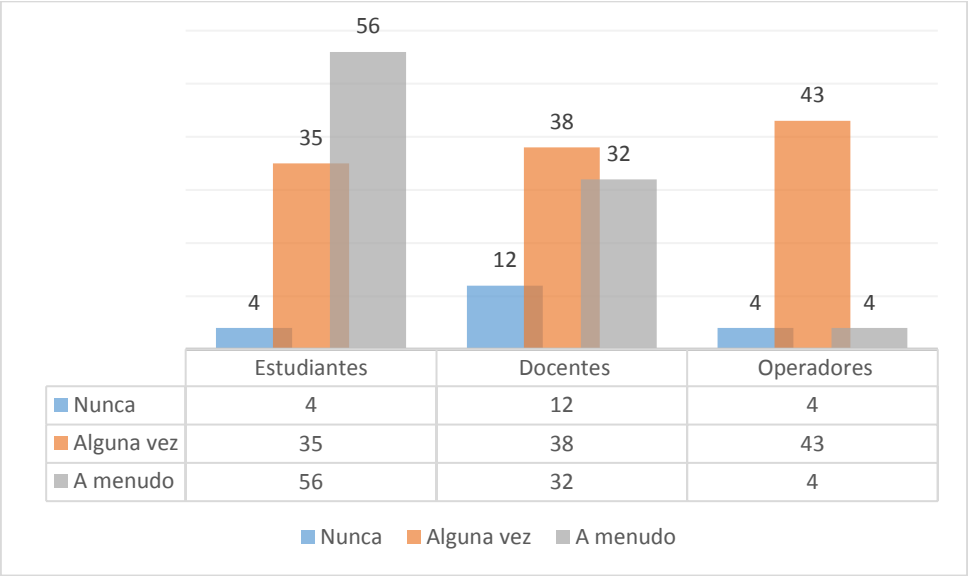


Gráfico 14 Pregunta respecto al Objetivo de Control A9. Control de acceso
Elaborado por: La Investigadora

Análisis: 20 encuestados equivalente al 8,55% manifiesta no haber tenido nunca una dificultad para acceder al sistema. 116 equivalente al 50,88% indica haber tenido alguna vez una dificultad para acceder al sistema y 92 encuestados equivalente al 40,35% manifiesta tener a menudo dificultades para acceso al sistema.

Interpretación: Al menos un 40,35% de encuestados refiere tener a menudo dificultades de acceso al sistema lo que podría evidenciar un problema en la disponibilidad de la información.

12. Motivo para tener dificultades de conexión

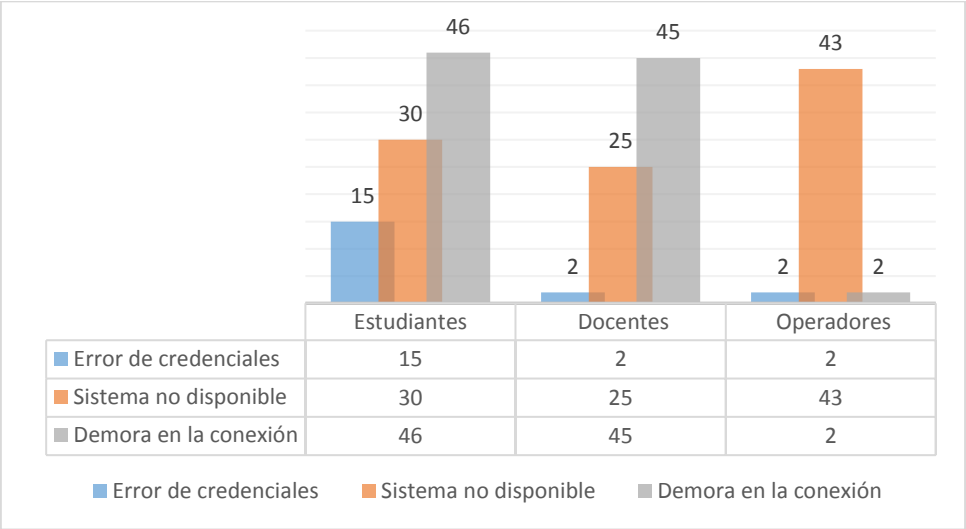


Gráfico 15 Pregunta respecto al Objetivo de Control A9. Control de acceso
Elaborado por: La Investigadora

Análisis: 19 encuestados equivalente al 9,05% manifiesta que la dificultad de acceso se ha ocasionado por error en el registro de credenciales de acceso. 98 equivalente al 46,67% indica que la dificultad se ha ocasionado porque el sistema no ha estado disponible. 93 equivalente al 44,29% manifiesta que la dificultad se ha ocasionado por demora en la conexión.

Interpretación: El 90,95% de encuestados manifiesta que las dificultades de acceso al sistema se han ocasionado por no estar el sistema disponible o demora en la conexión, lo cual evidencia una debilidad respecto a la disponibilidad de la información y la conexión multiusuario que admite el sistema de comunicaciones.

13. **¿Ha socializado sus credenciales de acceso con alguna otra persona?**

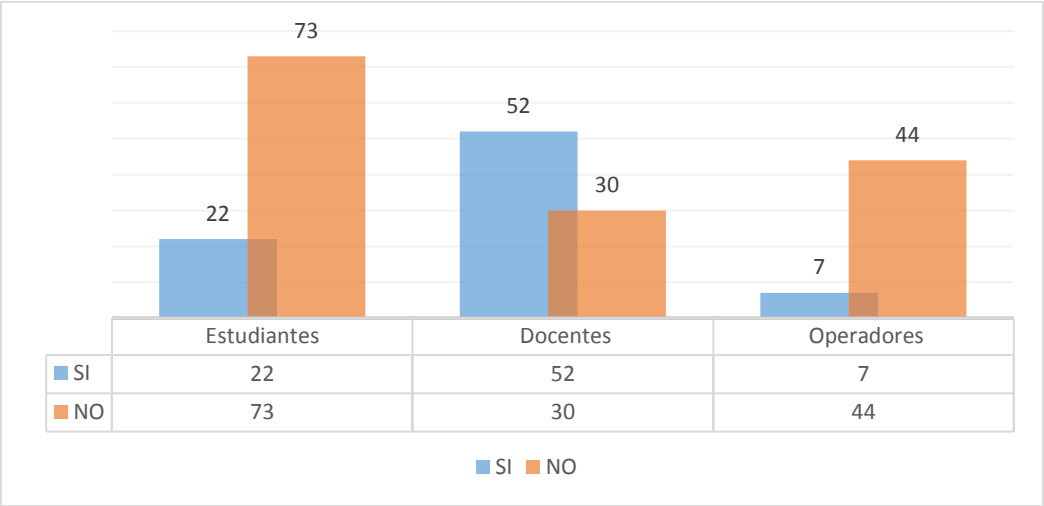


Gráfico 16 ¿Ha socializado sus credenciales de acceso con alguna otra persona?
Elaborado por: La Investigadora

Análisis: 81 encuestados equivalente al 35,53% manifiesta si haber socializado sus credenciales de acceso al sistema con otras personas. El 64,47% indica no haber socializado con nadie sus credenciales de acceso.

Interpretación: Un 35,53% de usuarios que han socializado sus credenciales de acceso con otras personas manifiesta haberlo hecho por necesidad de ayuda para registro de información. Este particular se presenta principalmente en el personal docente que utiliza la ayuda de estudiantes para registrar la información de asistencia y calificaciones en el sistema académico. Esto denota que la falta de capacitación sobre seguridad puede poner en riesgo la integridad de la información.

Conclusiones

De los resultados obtenidos de las encuestas aplicadas a los usuarios y operadores del sistema académico se puede concluir que el recurso humano constituye una arista muy importante dentro del proceso de seguridad; y por lo tanto requiere una especial atención para fortalecer su capacidad de operación.

Se requiere robustecer los procesos de capacitación, acuerdos de confidencialidad, procedimientos de desvinculación laboral que garanticen la inhabilitación de usuarios, directrices respecto a las vulnerabilidades técnicas de los equipos que utilizan los usuarios para acceder al sistema académico y responsabilidad de los usuarios respecto a la seguridad de la información a la que acceden y manipulan.

La institución debe canalizar esfuerzos para capacitar a los usuarios en materia de seguridad de la información, emitir recomendaciones respecto a las vulnerabilidades técnicas de los equipos, protección contra malware, procesos de inicio y cierre seguro de sesiones, confidencialidad respecto a la información que se manipula y concienciación sobre la responsabilidad de notificar cuando se detecta una vulnerabilidad en el proceso de acceso y manejo de información.

- Respecto al punto 2. De la auditoría aplicada con cada uno de los objetivos y controles de seguridad que establece la norma NTE INEN/ISO 27001:2013, se han obtenido los siguientes resultados, respecto al nivel de madurez:

1. ***Nivel de madurez Objetivo A5 Política de seguridad de la información***

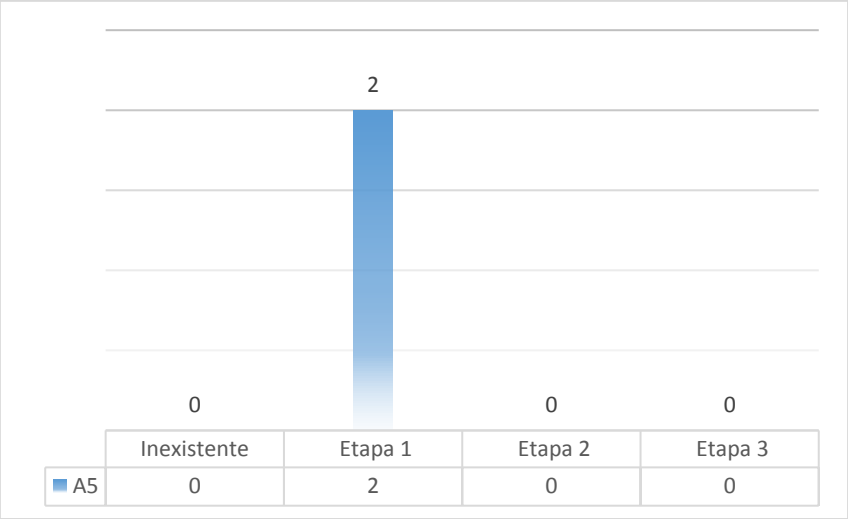


Gráfico 17 Madurez Política de seguridad de la información
Elaborado por: La Investigadora

Análisis: De los 2 controles que conforman el objetivo ***Política de seguridad de la información***, los 2 equivalente al 100% se encuentran en etapa 1 de madurez.

Interpretación: Los controles del Objetivo de Seguridad A5 se encuentran en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales (roles y privilegios de acceso, seguridad física de los servidores, protección contra malware, gestión de vulnerabilidades técnicas), pero no de forma documentada o sistemática. lo cual puede resultar insuficiente en algún determinado momento al no ser un procedimiento formalmente establecido.

2. *Nivel de madurez Objetivo A6 Organización Seguridad de la Información*

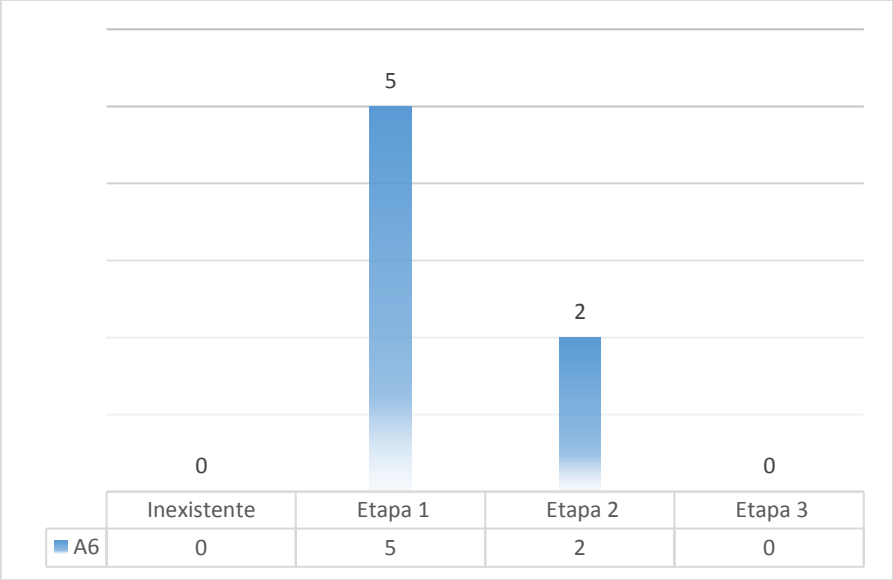


Gráfico 18 Madurez Organización Seguridad de la Información
Elaborado por: La Investigadora

Análisis: De los 7 controles que conforman el Objetivo ***Seguridad de la Información***, 5 equivalente al 71,43% se encuentra en etapa 1 de madurez, y 2 equivalente al 28,57 en etapa 2 de madurez.

Interpretación: Cinco controles del objetivo de seguridad A6 se encuentran en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales (roles y privilegios, custodios respecto a los activos hardware, coordinación interna en caso de incidentes). Dos controles se encuentran en etapa 2 de madurez, es decir que se cuenta con evidencia documental o el proceso informal ya es repetitivo (trabajo colaborativo con el CSIT de CEDIA, manejo de VPN's).

3. *Nivel de madurez Objetivo A7 Seguridad en Recursos Humanos*

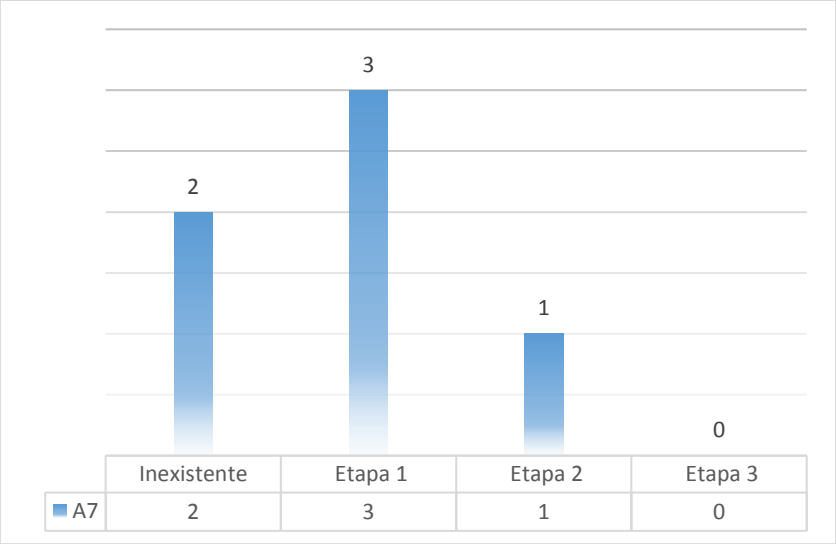


Gráfico 19 Madurez Seguridad en Recursos Humanos
Elaborado por: La Investigadora

Análisis: De los 6 controles que conforman el objetivo ***Seguridad*** **en Recursos Humanos,** 2 equivalente al 33,33% no han sido implementados, 3 equivalente al 50% se encuentran en etapa 1 de madurez, y 1 equivalente al 16,67 se encuentra en etapa 2 de madurez.

Interpretación: Dos controles del objetivo A7 no han sido implementados (capacitación a usuarios respecto a seguridad, procesos disciplinarios). Tres se encuentran en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales respecto a la seguridad (asignación de responsabilidades a técnicos y operadores, procedimiento de inhabilitación de credenciales previa desvinculación laboral). Uno en etapa 2 de madurez, es decir que se cuenta con evidencia documental o el procedimiento informal ya es repetitivo (selección de personal conforme directrices establecidas por Talento Humano).

4. Nivel de madurez Objetivo A8 Gestión de Activos

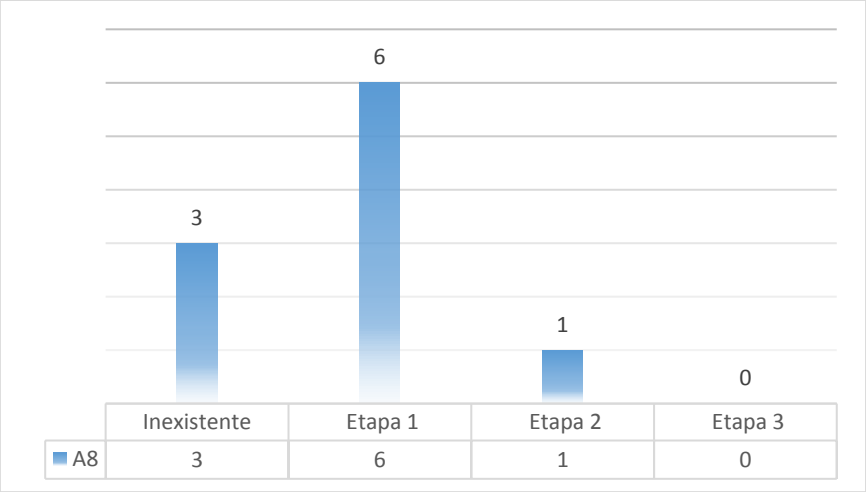


Gráfico 20 Madurez Gestión de Activos
Elaborado por: La Investigadora

Análisis: De los 10 controles que conforman el objetivo ***Gestión de Activos,*** 3 controles, equivalente al 30% no han sido implementados, 6 equivalente al 60% se encuentran en etapa 1 de madurez y 1 equivalente al 10% en etapa 2 de madurez.

Interpretación: Tres controles del objetivo A8 no han sido implementados (inventario de activos de información, clasificación y etiquetado de información en función de la sensibilidad y criticidad). Seis controles se encuentran en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales respecto a la seguridad (Custodios de activos hardware, indicaciones generales a usuarios respecto a cuidado de claves de acceso, manejo de información en medios extraíbles depende del comprometimiento del personal técnico que la maneja). Un control se encuentra en etapa 2 de madurez, es decir que se cuenta con evidencia documental (Estándar TIER capa 2 para el Data Center).

5. Nivel de madurez Objetivo A9 Control de Acceso

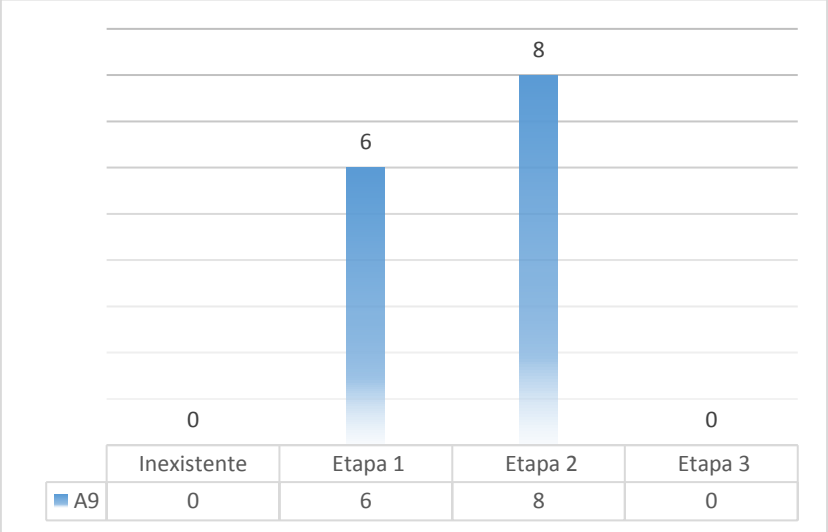


Gráfico 21 Madurez Control de Acceso
Elaborado por: La Investigadora

Análisis: De los 14 controles que conforman el objetivo ***Control de acceso,*** 6 equivalente al 42,86% se encuentra en etapa 1 de madurez y ocho equivalente s al 57,14% en etapa 2 de madurez.

Interpretación. Seis controles del objetivo A9 se encuentran en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales respecto a la seguridad (procedimientos no formales para la creación, inhabilitación y eliminación de usuarios, separación de redes de comunicaciones por tipo de usuario, monitoreo de tráfico de red, proceso de validación para acceso a red inalámbrica, procedimientos de seguridad respecto a longitud de contraseñas y aceptación de caracteres especiales). Ocho controles se encuentran en etapa 2 de madurez, es decir que se cuenta con evidencia documental o el procedimiento informal ya es repetitivo (privilegios específicos respecto a DDL y DML, acceso por roles, formulario para inhabilitación de usuarios por desvinculación laboral, activación de credenciales previa capacitación a operadores, seguridades a nivel de red inalámbrica, hash criptográfico para contraseñas).

6. Nivel de madurez Objetivo A10 Criptografía

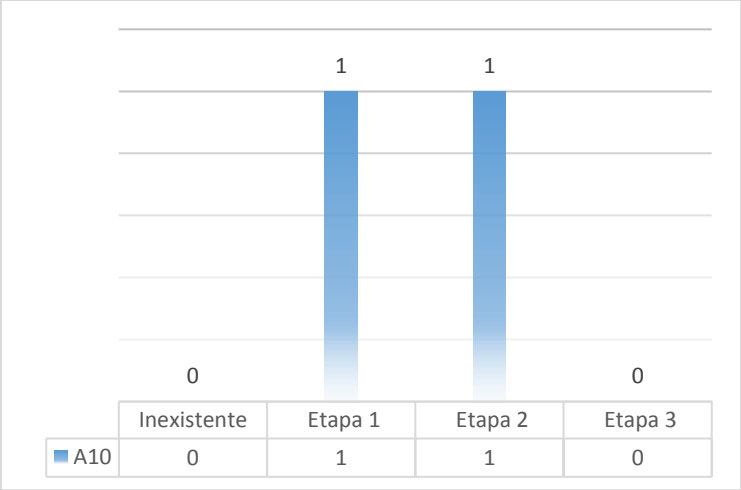


Gráfico 22 Madurez Criptografía
Elaborado por: La Investigadora

Análisis: De los 2 controles del objetivo ***Criptografía,*** uno equivalente al 50% se encuentran en etapa 1 de madurez y uno equivalente al 50% se encuentra en etapa 2 de madurez.

Interpretación: Un control del objetivo de seguridad A10 se encuentran en etapa 1 de madurez, es decir que se han implementado esfuerzos puntuales, pero no de forma documentada (Protocolos de seguridad para WLAN, hash criptográfico para contraseñas. No está documentada la política), Un control se encuentra en etapa 2 de madurez, es decir que se cuenta con evidencia documental o el procedimiento informal ya es repetitivo (certificado digital para la plataforma UVirtual).

7. Nivel der madurez Objetivo A11 Seguridad Física y del entorno

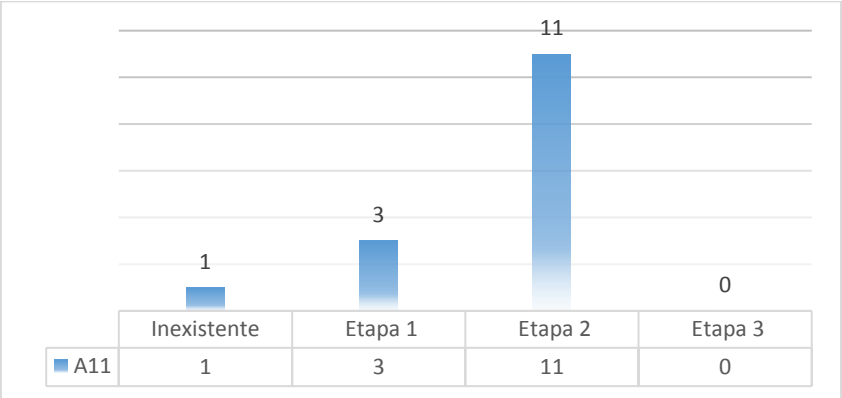


Gráfico 23 Madurez Seguridad Física y del entorno
Elaborado por: La Investigadora

Análisis: De los 15 controles que conforman el objetivo de ***Seguridad Física y del entorno,*** 1 equivalente al 6,67% no ha sido implementado, 3 equivalente al 20% se encuentran en etapa 1 de madurez y 11, equivalente al 73,33% en etapa 2 de madurez.

Interpretación: Un control del objetivo A11 no ha sido implementado (control de entrada y salida de activos de información). Tres controles se encuentran en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales (equipo multidisciplinario para evaluación de emergencias y desastres, activos hardware con custodio sin políticas de protección, directrices generales sobre cierre de sesiones a usuarios en procesos de capacitación). 11 controles en etapa 2 de madurez, es decir que se cuenta con evidencia documental o el procedimiento informal ya es repetitivo (Estándar TIER 2 para el Data Center y restricciones y control de acceso mediante control biométrico, diseño estructural antisísmico, cumplimiento de estándares de seguridad eléctrico, contraincendios, hidrosanitario, control de ingreso y materiales admitidos al área de servidores, plan de mantenimiento de redes e infraestructura, equipos protegidos por contraseña)

8. Nivel de madurez Objetivo A12 Seguridad de las Operaciones

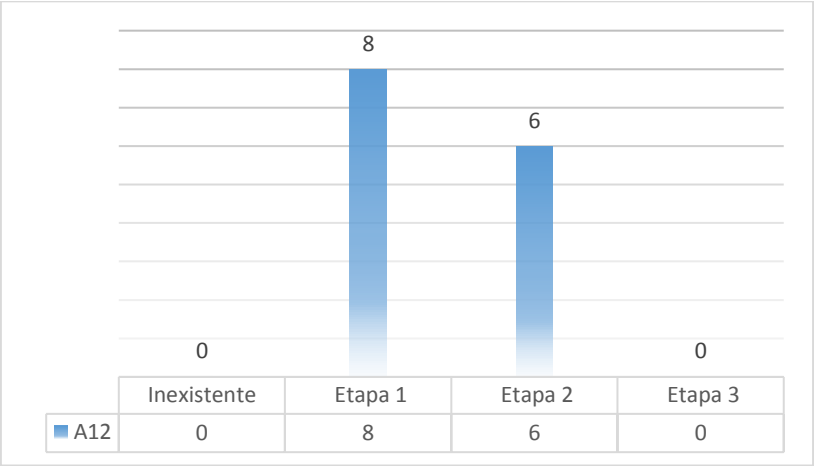


Gráfico 24 Madurez Seguridad de las Operaciones
Elaborado por: La Investigadora

Análisis: De los 14 controles que conforman el objetivo ***Seguridad de las Operaciones,*** 8 equivalente al 57,14% se encuentra en etapa 1 de madurez y 6 equivalente al 42,86% en etapa 2 de madurez.

Interpretación: 8 controles del objetivo A12 se encuentran en etapa 1 de madurez, es decir que se han implementado esfuerzos puntuales respecto a la seguridad (manuales técnicos y de usuario respecto a los activos software y algunos respecto a activos hardware, pruebas funcionales previo poner un sistema en producción, no se supervisa trabajo de técnicos y operadores, pero se maneja privilegios de acceso, actualización de sistema operativos). 6 controles se encuentran en etapa 2 de madurez, es decir que se cuenta con evidencia documental o el proceso informal ya es repetitivo (manejo de ambientes separados y credenciales diferentes para sistemas en desarrollo, pruebas y producción, congelamiento de equipos de operadores, auditoría de transacciones.

9. Nivel de madurez Objetivo A13 Seguridad en las Comunicaciones

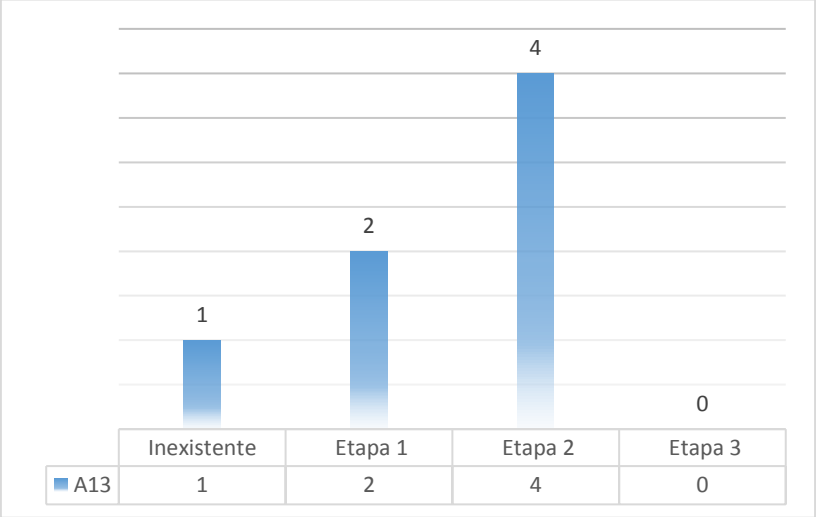


Gráfico 25 Madurez Seguridad en las Comunicaciones
Elaborado por: La Investigadora

Análisis: De los 7 controles que conforman el objetivo ***Seguridad en las Comunicaciones,*** 1 equivalente al 14,29% no ha sido implantado; 2 equivalente al 28,57% se encuentran en etapa 1 de madurez y 4 equivalente al 57,14% en etapa 2 de madurez.

Interpretación: Un control del objetivo de seguridad A13 no ha sido implementado (política que regule la transferencia de información por mensajería electrónica). 2 controles se encuentran en etapa 1 de madurez, es decir que se han implementado esfuerzos puntuales respecto a la seguridad (no está clasificada la información por su nivel de sensibilidad, en etapa de implantación acuerdos de confidencialidad para operadores y usuarios). 4 controles se encuentran en etapa 2 de madurez, es decir que se cuenta con evidencia documental o el proceso informal es repetitivo (Monitoreo de vulnerabilidades con colaboración de CSIT de CEDIA, protocolo AES para WLAN).

10. *Nivel de madurez Objetivo A14 Adquisición, mantenimiento y desarrollo de sistemas*

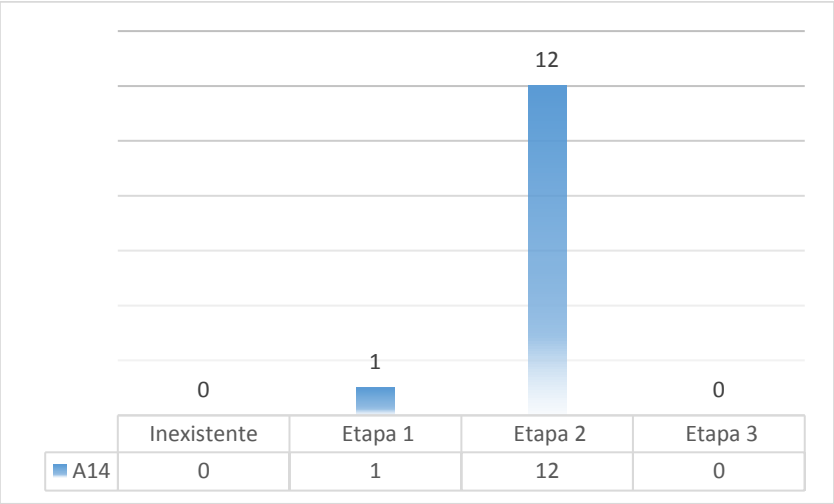


Gráfico 26 Madurez Adquisición, mantenimiento y desarrollo de sistemas
Elaborado por: La Investigadora

Análisis: De los 13 controles que conforman el objetivo ***Adquisición, mantenimiento y desarrollo de sistemas,*** 1 control equivalente al 7,69% se encuentra en etapa 1 de madurez y 12 equivalente al 92,31% en etapa 2 de madurez.

Interpretación: Un control del objetivo de seguridad A14 se encuentra en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales respecto a la seguridad (procedimientos de adquisición respecto a términos de referencia). 12 controles se encuentran en etapa 2 de madurez, es decir que se cuenta con evidencia documental o el proceso informal ya es repetitivo (seguridad a nivel de aplicación en proyectos nuevos, sha criptográfico, codificación AES para WLAN, certificado digital para UVirtual, control de cambios, análisis de riesgos y pruebas funcionales en proyectos de desarrollo).

11. Nivel de madurez Objetivo A15 Relación con proveedores

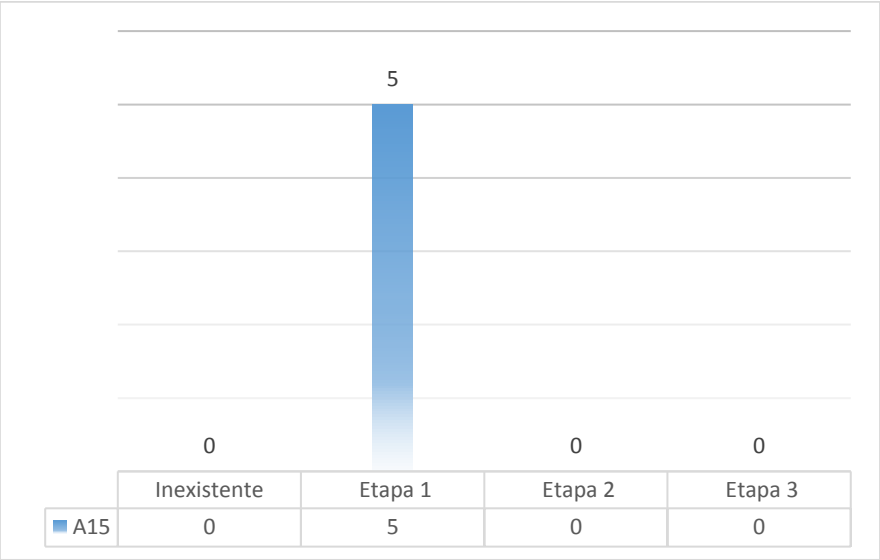


Gráfico 27 Madurez Relación con proveedores
Elaborado por: La Investigadora

Análisis: De los 5 controles que conforman el objetivo ***Relación con proveedores,*** los 5 equivalente al 100% se encuentran en etapa 1 de madurez.

Interpretación: Los 5 controles del objetivo A15 se encuentran en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales respecto a la seguridad (cumplimiento ley de contratación pública, relación contractual con base a términos de referencia), lo cual puede llegar a ser insuficiente en determinado momento porque no es un procedimiento formalmente instaurado, se cumplen únicamente conforme la normativa legal vigente. No existe una adaptación a nivel institucional.

12. Nivel de madurez Objetivo A16 Gestión Incidentes de seguridad

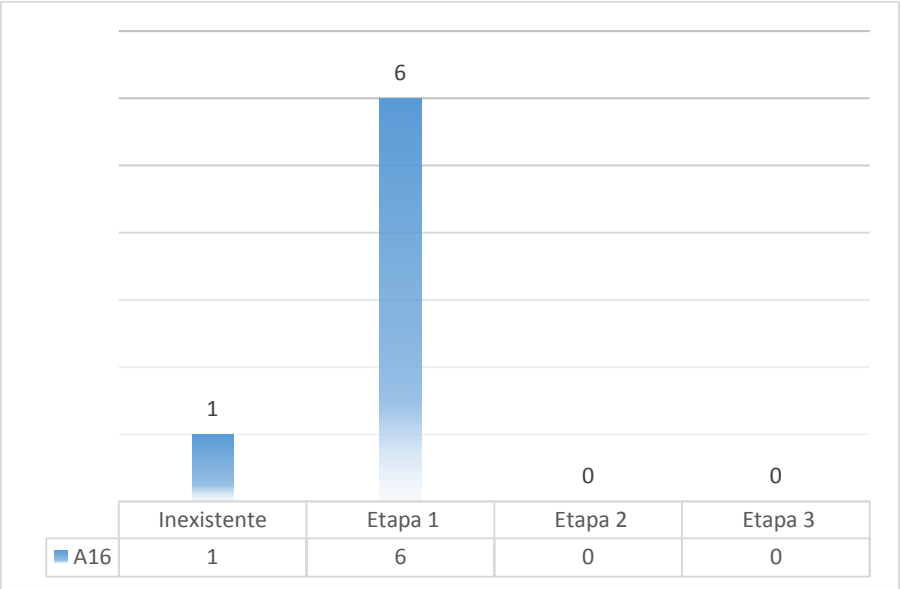


Gráfico 28 Madurez Gestión Incidentes de seguridad
Elaborado por: La Investigadora

Análisis: De los 7 controles que conforman el objetivo ***Gestión de Incidentes de seguridad,*** 1 equivalente al 14,29% no ha sido implementado y 6 equivalente al 85,71% se encuentran en etapa 1 de madurez.

Interpretación: Un control del objetivo A16 no ha sido implementado (concienciación a usuario para informar vulnerabilidades detectadas). 5 controles se encuentran en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales (detección de eventos de seguridad en colaboración con CSIRT de CEDIA, se toman acciones conforme se presenten los eventos de seguridad), lo cual puede resultar insuficiente en determinado momento al no ser un proceso formalmente establecido, monitoreado y mejorado.

13. *Nivel de madurez Objetivo A17 Gestión de la continuidad de la seguridad*

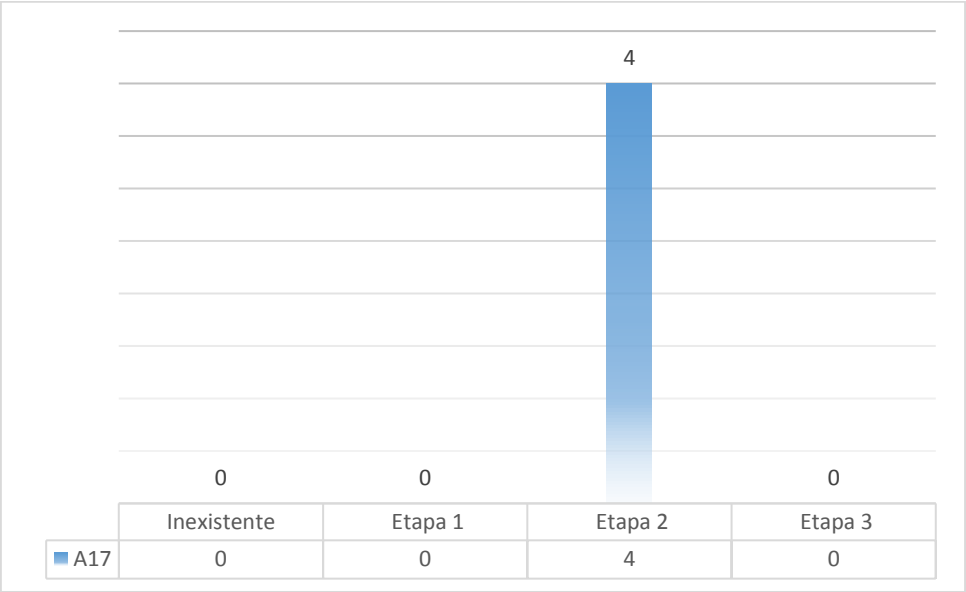


Gráfico 29 Madurez Gestión de la continuidad de la seguridad
Elaborado por: La Investigadora

Análisis: De los 4 controles que conforman el objetivo ***Gestión de la seguridad,*** 4 equivalente al 100% se encuentran en etapa 2 de madurez.

Interpretación: Los cuatro controles del objetivo A17 se encuentra en etapa 2 de madurez, es decir que se cuenta con evidencia documental o el proceso informal ya es repetitivo (designados responsables para mitigar eventos de seguridad, estándar TIER II para Data Center, redundancia en las comunicaciones).

14. Nivel de madurez Control A18 Cumplimiento

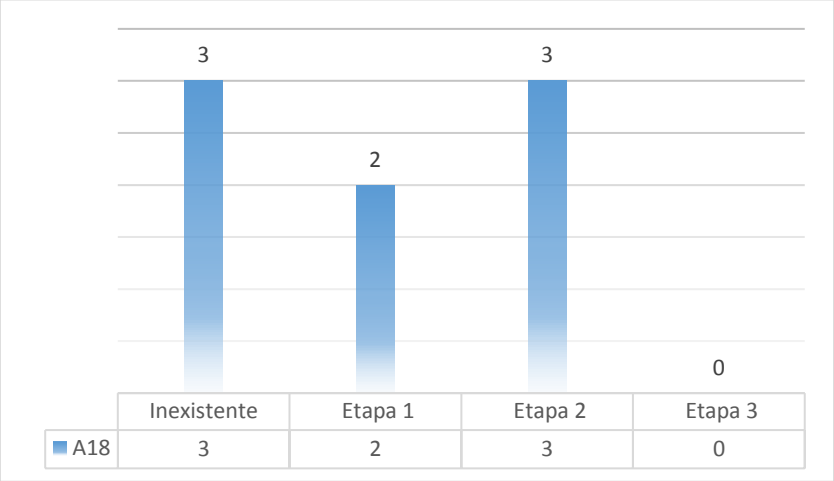
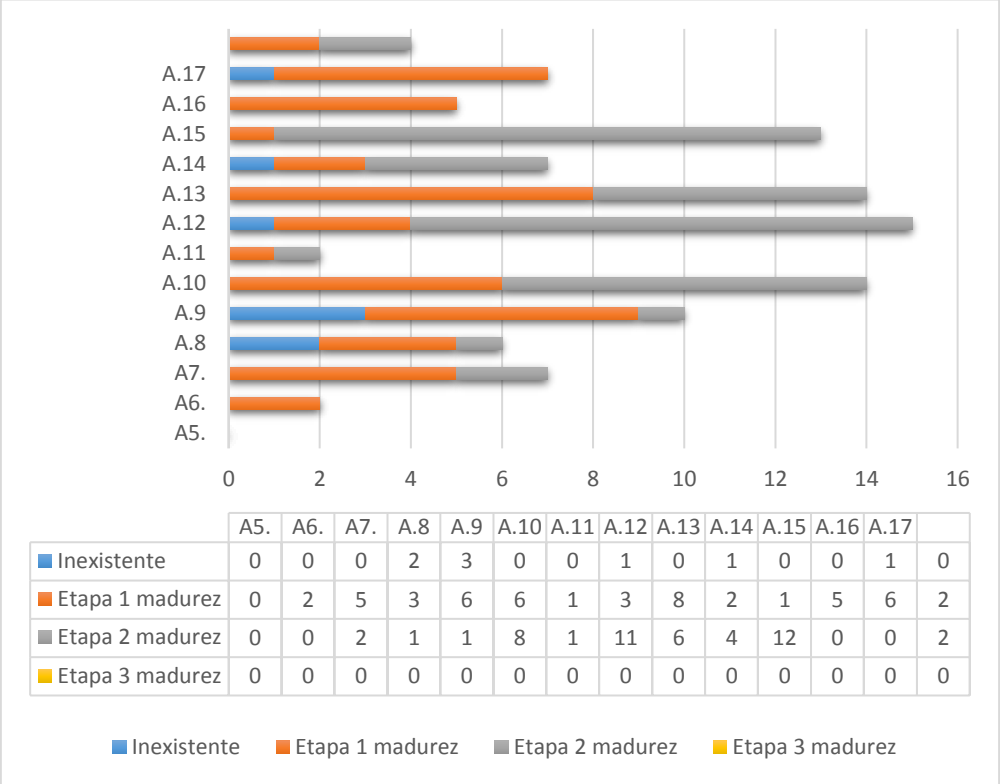


Gráfico 30 Madurez Cumplimiento
Elaborado por: La Investigadora

Análisis: De los 8 controles que conforman el objetivo ***Cumplimiento,*** 3 controles equivalente al 37,50% no han sido implementados, 2 equivalente al 25% se encuentran en etapa 1 de madurez y 3 equivalente al 37,50% se encuentran en etapa 2 de madurez.

Interpretación: 3 controles del objetivo A18 no han sido implementados (Identificación y clasificación de los registros de información). 2 controles se encuentran en etapa 1 de madurez, es decir se han implementado esfuerzos puntuales respecto a la seguridad (acuerdos de confidencialidad con operadores y usuarios, cumplimiento técnico de los sistemas conforme demanda). 3 controles se encuentran en etapa 2 de madurez, es decir que se cuenta con evidencia documentada o el procedimiento formal ya es repetitivo (normativa legal interna y externa respecto al giro del negocio, código fuente registrado en el IEPI, protección de derechos de autor, contratación de licencias de software propietario, sha criptográfico y certificado digital para la plataforma UVirtual).

15. Nivel de madurez por Objetivo de Control



	A5.	A6.	A7.	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	
Inexistente	0	0	0	2	3	0	0	1	0	1	0	0	1	0
Etapa 1 madurez	0	2	5	3	6	6	1	3	8	2	1	5	6	2
Etapa 2 madurez	0	0	2	1	1	8	1	11	6	4	12	0	0	2
Etapa 3 madurez	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Gráfico 31 Madurez por Objetivo de Control
Elaborado por: La Investigadora

Análisis: De los 14 objetivos de control que establece la norma 27001, 11 controles equivalente al 9,65% no han sido implementados, 52 equivalente al 45,61%, se encuentran en etapa 1 de madurez, 51 equivalente al 44,74% se encuentran en etapa 2 de madurez. Ningún control registra etapa 3 de madurez.

Interpretación: El 9.65% de controles de seguridad no han sido implementados. El 45,61% de controles de seguridad se cumplen por esfuerzos puntuales respecto a la seguridad. El 44,74% ya cuentan con evidencia documental o es un proceso repetitivo que además se adapta a las regulaciones legales. Ningún control de seguridad cuenta con un procedimiento formalmente establecido que permita su planificación, monitoreo y mejora.

Conclusiones:

La institución ha implementado esfuerzos puntuales respecto a la seguridad de la información, mismos que se basan en el conocimiento del personal técnico, el aprendizaje respecto a incidentes de seguridad y el compromiso personal del equipo técnico por mejorar los servicios. También existe cumplimiento de normativa legal (respecto a la cual se va adaptando los procedimientos para su acatamiento.

Lo antes manifestado es un escenario aceptable cuando el manejo de información a través de redes comunicaciones y bases de datos, recién inicia; sin embargo, esto resulta insuficiente cuando los sistemas van en crecimiento, considerando que el nivel de vulnerabilidad, criticidad e impacto de la información crece aceleradamente, por lo tanto, no se puede seguir trabajando respecto a la mitigación de incidentes, sino sobre su prevención.

Se puede observar que a pesar de que existen muchos controles que han alcanzado una etapa 2 de madurez, mientras no se cuente con un procedimiento implementado y documentado que permita el monitoreo, evaluación y mejora respecto a la seguridad, los activos de información están expuestos a un riesgo potencialmente grave que es la incertidumbre, ya que al no tener identificados los puntos críticos de gestión, no se puede saber de dónde puede venir un ataque y el consecuente impacto en la pérdida de confidencialidad, integridad y disponibilidad de la información, así como los costos operativos y económicos que represente su recuperación.

- Respecto al punto 3. Para el análisis de la incidencia de la aplicación de normas ISO en instituciones de Educación Superior, se realizó una comparativa entre los resultados obtenidos por investigaciones aplicadas en otras IES (2.1.1 Estado del Arte), y los resultados de la auditoría aplicada a la UNACH, así:

Tabla 6 Análisis incidencia normas ISO - Instituciones de Educación Superior

No	IES	Resultados	Conclusiones
1	Universidad de Colima – México	Certificada bajo la norma ISO 27001:2005, cuenta con 8 políticas de seguridad de la Información y un Comité del Sistema de Gestión Integral encargado de la implementación, monitoreo y evaluación del cumplimiento de la norma. Universidad de Colima. (2017)	Etapa 3 de madurez. Está implementado un control documentado respecto a la seguridad de la información, su monitoreo, tratamiento y mejora. Ha alcanzado el nivel de certificación en seguridad.
2	Universidad Central del Ecuador	Estudio con base a la Norma ISO 27001:2005: 7 objetivos de control con un insuficiente nivel de madurez y 4 con un nivel suficiente de madurez. Baldeón, M. y Guanopatín, J. (2015)	Etapa 1 de madurez. Se han implementado esfuerzos puntuales respecto a la seguridad, pero no de forma documentada o sistemática que permita su monitoreo, tratamiento y mejora.
3	Universidad Politécnica Salesiana Sede Quito Campus Sur	Estudio con base a la Norma ISO 27001:2005: Identificación y valoración de activos de información y análisis de amenazas. Tixilima, V (2015).	Etapa 1 de madurez. Se han implementado esfuerzos puntuales respecto a la seguridad, pero no de forma documentada o sistemática que permita su monitoreo, tratamiento y mejora.
4	Universidad Nacional de Loja	Estudio con base a la Norma ISO 27001:2005: Identificación de la infraestructura hardware y red de comunicaciones. Soluciones para prevenir materialización de riesgos de seguridad. Torres, H (2010).	Etapa 1 de madurez. Se han implementado esfuerzos puntuales respecto a la seguridad, pero no de forma documentada o sistemática que permita su monitoreo, tratamiento y mejora.
5	Universidad Nacional de Chimborazo	Auditoría con base a las normas NTE INEN ISO/IEC 27001:2013 y 27002:2013 Evaluación del nivel de madurez respecto a los 114 controles de seguridad que establece la norma. 9,65% de controles no implementados. 45,61% de controles en etapa 1 de madurez 54,74% de controles en etapa 2 de madurez Ningún control en etapa 3 de madurez.	Etapa 1 de madurez. Se han implementado esfuerzos puntuales respecto a la seguridad, pero no de forma documentada o sistemática que permita su monitoreo, tratamiento y mejora.

Fuente: Estado del arte de esta investigación y auditoria a la UNACH
Elaborado por: La Investigadora

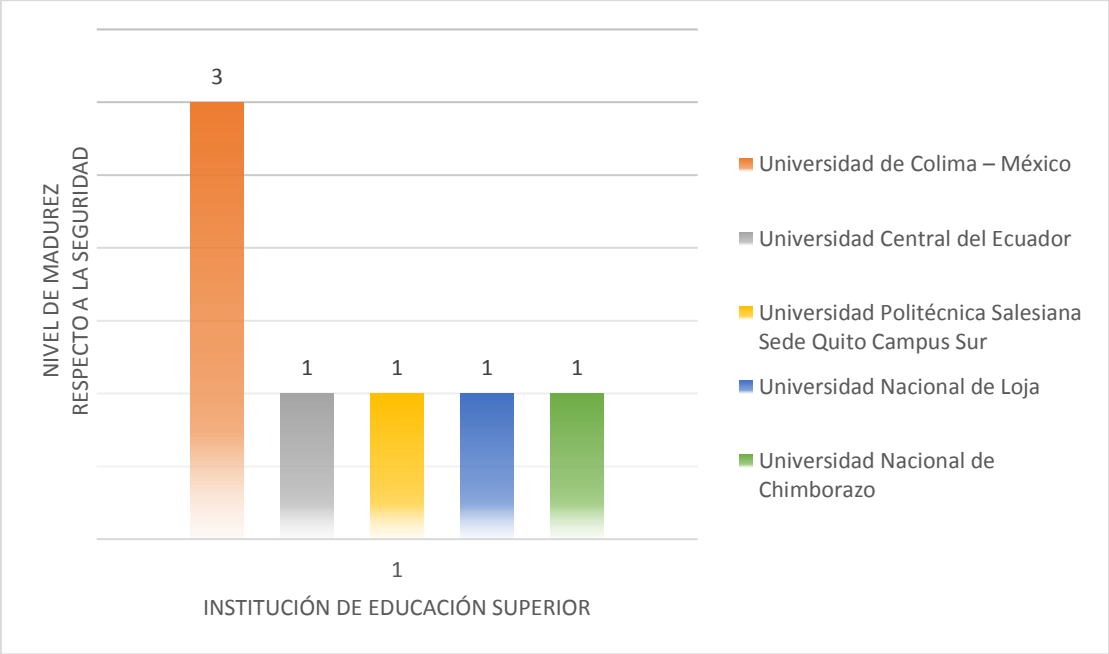


Gráfico 32 Madurez en seguridad IES analizadas
Elaborado por: La Investigadora

Análisis: De las 5 Instituciones de Educación Superior analizadas sobre su nivel de madurez respecto a la seguridad de la información, 1 equivalente al 20% se encuentra en etapa 3 de madurez y 4 equivalente al 80% se encuentran en etapa 1 de madurez.

Interpretación: Una IES (Colima – México) ha alcanzado el nivel 3 de madurez considerando que ha implementado políticas de seguridad y un comité encargado de su monitoreo, evaluación y cumplimiento, por lo que sus procesos han sido certificados bajo la norma internacional ISO 27001:2005.

Las cuatro IES (UCE, UPS Quito Campus Sur, UNL, UNACH – Ecuador) se encuentran en promedio en etapa 1 de madurez, es decir que se han implementado esfuerzos puntuales respecto a la seguridad, pero no se cuenta con un procedimiento formal, documentando y sistemático que garantice el monitoreo, evaluación mejora y continuidad de la seguridad de la información.

Conclusiones:

Se puede observar que existe una relación directa entre la implementación de procedimientos sistemáticos y formales que se orienten a gestionar la seguridad de la información, y el nivel de madurez alcanzado respecto a dicha seguridad, reconociendo una vez más que no es suficiente con implementar esfuerzos puntuales o de mitigación, el trabajo debe orientarse a la gestión de procesos metódicos de prevención en materia de seguridad.

4.2 Verificación de la hipótesis

Planteamiento

Hipótesis Nula

Ho: Las normas ISO 27001 y 27002 NO inciden en la seguridad de la información.

Hipótesis Alterna

Hi: Las normas ISO 27001 y 27002 SI inciden en la seguridad de la información.

Método utilizado

Para verificar la hipótesis se utiliza el método estadístico X^2 (Ji- Cuadrado), que es una prueba no paramétrica (porque los datos no se ajustan a una distribución conocida), que permite establecer la relación entre dos variables, así:

- La hipótesis nula demuestra que no hay dependencia entre las variables, es decir son independientes la una de la otra.

- La hipótesis alterna demuestra que no hay independencia entre las dos variables, es decir está relacionada la una a la otra.

La fórmula de Ji – Cuadrado (X^2) se obtiene así:

$$x^2 = \sum \frac{(\text{frecuencia observada} - \text{frecuencia esperada})^2}{\text{frecuencia esperada}_i}$$

Nivel de significancia

Se aplica un nivel de significancia de α = 0,05.

Grados de Libertad

v= (Cantidad de filas – 1) * (Cantidad de columnas – 1) = 52

Cálculos:

Frecuencia Observada

Tabla 7 Frecuencia Observada fo - Nivel de madurez - UNACH

Objetivo	Inexistente	Etapa 1	Etapa 2	Etapa 3	Total
	Bajo	Medio	Alto	Excelente	
A5	0	2	0	0	2
A6	0	5	2	0	7
A7	2	2	2	0	6
A8	3	6	1	0	10
A9	0	6	8	0	14
A10	0	1	1	0	2
A11	1	3	11	0	15
A12	0	8	6	0	14
A13	1	2	4	0	7
A14	0	1	12	0	13
A15	0	5	0	0	5
A16	1	6	0	0	7
A17	0	0	4	0	4
A18	3	2	3	0	8
TOTAL	**11**	**50**	**53**	**0**	**114**

Fuente: Auditoría UNACH
Elaborado por: La Investigadora

Frecuencia Esperada

La frecuencia esperada ***fe*** se calcula a través del producto de los totales marginales (total de la fila x total de la columna), dividido por el número total de casos (gran total):

$$\text{fe} = \frac{(\text{total de la fila})\text{x}\ (\text{total de la columna})}{\text{gran total}}$$

Prueba de la hipótesis

Tabla 8 Prueba de la Hipótesis

Objetivo	Inexistente / Bajo		Etapa 1 / Medio		Etapa 2 / Alto		Etapa 3 / Excelente		$(fo-fe)^2/fe$
	fo	fe	fo	fe	fo	fe	fo	fe	
A5	0	0.19	2	0.88	0	0.91	0	0.02	0.19
A6	0	0.68	5	3.07	2	3.19	0	0.06	0.68
A7	2	0.58	2	2.63	2	2.74	0	0.05	3.49
A8	3	0.96	6	4.39	1	4.56	0	0.09	4.29
A9	0	1.35	6	6.14	7	6.39	1	0.12	1.35
A10	0	0.19	1	0.88	1	0.93	0	0.02	0.19
A11	1	1.45	3	6.58	11	6.84	0	0.13	0.14
A12	0	1.35	8	6.14	6	6.39	0	0.12	1.35
A13	1	0.68	2	3.07	4	3.19	0	0.06	0.16
A14	0	1.25	1	5.70	12	5.93	0	0.11	1.25
A15	0	0.48	5	2.19	0	2.28	0	0.04	0.48
A16	1	0.68	6	3.07	0	3.19	0	0.06	0.16
A17	0	0.39	0	1.75	4	1.82	0	0.04	0.39
A18	3	0.77	2	3.51	3	3.65	0	0.07	6.43
X^2 Ji - Cuadrado									**20.55**

Elaborado por: La Investigadora

Criterio:

Se rechaza la hipótesis nula si $X^2 < \alpha$

Valores X^2 para 52 grados de Libertad					
	Probabilidad de un valor superior a α				
	0,01	**0,05**	0,10	0,20	0,25
52	31,25	**36,44**	39,43	43,28	44,81

Obtenido el resultado de X^2 20.55 < 36.44, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis de investigación (Hi), esto es: Las normas ISO 27001 y 27002 SI inciden en la seguridad de la información.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- A pesar de que el recurso humano cumple un rol fundamental dentro del proceso de seguridad de la información, pocos esfuerzos de capacitación y concienciación se han planificado.
- La capacitación, definición de responsabilidades y políticas claras respecto al acceso y manipulación de datos, es fundamental para una adecuada gestión de la información.
- En materia de seguridad, al no trabajar en prevención, las instituciones arriesgan sus activos de información, estando estos expuestos a amenazas que pueden afectar la confidencialidad, integridad y disponibilidad.
- La evidencia obtenida de la auditoría permite corroborar que los esfuerzos puntuales respecto a la seguridad de la información no son suficientes; por lo que, la institución debe dar un paso más allá y pensar en una verdadera gestión respecto a la seguridad, basada en los principios de planeación, monitoreo, evaluación y mejora, que garanticen su continuidad y la protección de los activos.
- El no planificar una gestión de seguridad con base a la prevención en lugar de únicamente la mitigación, conlleva a ubicar a los activos de información en un alto nivel de inseguridad, cuyas amenazas pueden provenir desde diferentes fuentes con o sin la intención de provocar daño; las cuales pueden convertirse en un incidente de seguridad que ocasione altos costos operativos y económicos para su recuperación.
- La información obtenida respecto a las IES investigadas, permite evidenciar que existe una correlación entre una gestión sistemática de la seguridad de la información, basada en políticas y procedimientos

formales que abarquen todas las áreas involucradas, en contraposición al trabajo sobre demanda, es decir ir cubriendo brechas de seguridad a medida que se presenten incidentes.

- Respecto a las Instituciones de Educación Superior investigadas, se puede concluir que una IES ha implementado un sistema de gestión de seguridad de la información e incluso ha certificado sus procesos; mientras que, las otras cuatro han implementado en promedio medidas básicas de seguridad, pero no cuentan con procedimientos formalmente establecidos que permitan su monitoreo, evaluación y mejora.
- Lo anterior desencadena en que la seguridad de la información dependa de las acciones posteriores a un incidente de seguridad o a la buena predisposición del personal de tecnología por mejorar dicha seguridad y no a un procedimiento planificado de gestión.
- Estos resultados permiten evidenciar que no existe una adecuada seguridad respecto a la información contenida en las bases de datos, por lo que la aplicación de las normas 27001 y 27002 SI incide en la seguridad de las mismas.

5.2 Recomendaciones

- Implementar planes de capacitación y concienciación respecto a la seguridad de la información para los usuarios de los sistemas de información.
- Considerando los resultados de la auditoría, se recomienda se proceda con la identificación y evaluación de los activos de información, proceso sistemático que debe formar parte de la gestión permanente de seguridad.
- La gestión de seguridad de la información debe ser considerada como un proceso sistematizado que contenga regulaciones, monitoreo, mejora y continuidad.
- Con base a los resultados de posicionamiento estratégico de los controles de seguridad (madurez vs importancia), la institución debe analizar los que puede priorizar para su implementación, considerando la disponibilidad económica, tiempo y recursos humanos requeridos. Lo citado se justifica considerando que el documento normativo, empleado para realizar la auditoría, considera la posibilidad de que las instituciones lo adapten a sus necesidades.
- Los puntos anteriores deben constituir el cimiento para la Gestión de la Seguridad de la información en la Unidad Técnica de Control Académico de la Universidad Nacional de Chimborazo con base en las normas NTE INEN ISO/IEC 27001 y 27002.

CAPÍTULO VI

DESARROLLO DE LA PROPUESTA

Gestión de Seguridad de la Información para la Unidad Técnica de Control Académico de la Universidad Nacional de Chimborazo

6.1 Datos Informativos

La Universidad Nacional de Chimborazo es una institución de educación superior, con personería jurídica, sin fines de lucro, autónoma, de derecho público, creada mediante Ley No. 98, publicada en el Suplemento del Registro Oficial No. 771, del 31 de agosto de 1995, su domicilio principal es la ciudad de Riobamba; sus siglas son UNACH. Se rige por la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior, su Reglamento, otras leyes conexas, su estatuto, los Reglamentos y Resoluciones que expidan el Consejo de Educación Superior; el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior; y, la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación y la Universidad. (Estatuto UNACH, 2013, pg. 1).

La Unidad Técnica de Control Académico es un organismo responsable del desarrollo de sistemas informáticos que permitan el control académico y administrativo, proporciona servicios de soporte, capacitación y asesoramiento técnico a todas las instancias que utilizan las aplicaciones informáticas desarrolladas por esta unidad.

Es la instancia institucional encargada del análisis, diseño e implementación de aplicaciones informáticas y de la administración de las bases de datos concernientes al control académico y a todos los servicios que se desprendan

de él, contribuyendo al cumplimiento de objetivos, misión y visión institucional. (Estatuto UNACH, 2013, pg. 36)

6.2 Antecedentes de la propuesta

Considerada la información como un activo de vital importancia para toda institución, la gestión de la seguridad que permita salvaguardar este recurso, es una tarea prioritaria que requiere del comprometimiento e inversión en tiempo y recursos por parte de los directivos institucionales.

En la Universidad Nacional de Chimborazo, conforme los resultados de la Auditoría a la seguridad de la información, se ha podido observar que el nivel de madurez general se encuentra en etapa 1, es decir que se han implementado mecanismos de seguridad puntuales o por sentido común.

Por lo antes expuesto se propone como base la implementación de políticas y procedimientos de seguridad que eleven sustancialmente el nivel de fiabilidad respecto a la seguridad de los sistemas de gestión de base de datos.

6.3 Justificación

Garantizar la calidad de información que maneja una institución, permite el desarrollo armónico de las actividades y la toma de decisiones de nivel estratégico, por lo que, invertir esfuerzos la confidencialidad, integridad y disponibilidad de la misma es una decisión acertada, cuyos frutos se pueden medir por el bajo nivel de incidentes de seguridad.

La información como activo y el intercambio de datos de forma síncrona, si bien han desarrollado de manera eficaz la forma de comunicarnos y transmitir información, no es menos cierto, que de forma equivalente se han multiplicado los riesgos y vulnerabilidades a las que está expuesta la misma.

En tal sentido en la actualidad no se puede dejar la seguridad de la información como un proceso secundario, de aplicación básica o de confianza en las buenas intenciones del personal, los usuarios y externos.

De allí la importancia de proponer una gestión de seguridad para la información que maneja la Unidad Técnica de Control Académico de la Universidad Nacional de Chimborazo, tomando como punto de partida los estándares NTE INEN ISO/IEC 27001:2013 y 27002:2013.

6.4 Objetivos

6.4.1 General

Implantar la gestión de seguridad de la información en la Unidad Técnica de Control Académico de la Universidad Nacional de Chimborazo, con base a las políticas y procedimientos que establecen las normas 27001 y 27002.

6.4.2 Específicos

- Identificar los activos de información de la Unidad Técnica de Control Académico de la Universidad Nacional de Chimborazo.
- Realizar el análisis estratégico de posicionamiento de los controles de seguridad en la Unidad Técnica de Control Académico de la UNACH, para priorizar los de urgente implementación.
- Establecer políticas de seguridad conforme el nivel de criticidad de los controles de seguridad.

- Sugerir el marco metodológico para la gestión de seguridad de la información.

6.5 Análisis de factibilidad

Tiene factibilidad operativa al tener la aprobación de la Unidad Técnica de Control Académico para analizar los procesos de seguridad de la información que se manejan.

Tiene factibilidad económica por cuanto los activos: infraestructura, software y bases de datos pertenecen a la institución, y sobre los mismos se planteará la gestión de seguridad.

Tiene factibilidad técnica por cuanto las Normas NTE INEN ISO/IEC 27000 proveen el marco regulatorio que facilita implantar buenas prácticas de seguridad.

Tiene factibilidad legal por cuanto la legislación ecuatoriana contempla en la Sección Tercera del Código Orgánico Integral Penal, lo siguiente: “Delitos contra la seguridad de los activos de los sistemas de información y comunicación Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años”. (COIP, 2014, art. 229).

De igual forma el subgrupo 410 Tecnología de la Información, de las Normas de Control Interno de la Contraloría General del Estado, establece las directrices que deben tomar en cuenta las entidades del sector público respecto a todos los procesos de acceso a la información como separación de funciones, plan estratégico, políticas, administración de proyectos, desarrollo y adquisición de software, adquisición y mantenimiento de infraestructura, seguridad, soporte técnico, monitoreo y capacitación entre otros. (Contraloría General del Estado. 2009, pg. 9, 68-75).

6.6 Fundamentación

Principio de Defensa en profundidad

Se refiere al diseño e implementación de varios niveles de seguridad que permita un mejor resguardo de la información, enfocándose tanto en la seguridad interna como la externa, conforme se visualiza en la Gráfico No. 6

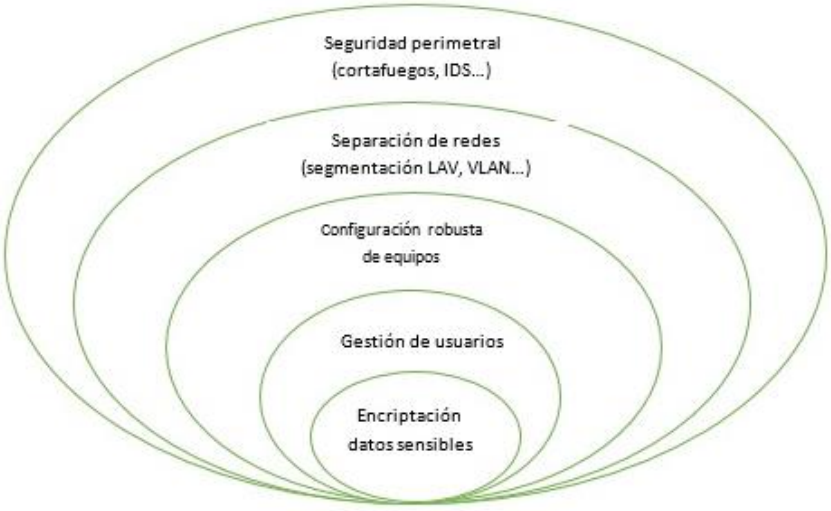


Gráfico 33 Principio de Defensa en Profundidad
Fuente: Gómez, A. (2011), pg. 52
Elaborado por: La Investigadora

Gestión de seguridad de la información

Es la parte del sistema general de gestión que se refiere a la política, estructura, recursos, procedimientos y procesos para implantar la seguridad de la información.

Considerando que no se puede hablar de una seguridad al 100%, por lo tanto, la fiabilidad del sistema de seguridad se basa en la metodología PDCA, así:

- Plan: selección y definición de medidas y procedimientos.
- Do: Implantación
- Check: Comprobación y verificación
- Act: Corrección de deficiencias detectadas.

Todo esto englobando al recurso humano, la tecnología, la legislación y la organización interna. (Gómez, A. 2011, pg. 52, 53, 54).

Amenaza

Cualquier evento con o sin intención que puede dañar los sistemas, causando pérdidas a la organización (Gómez, A. 2011, pg. 60).

Vulnerabilidad

Es una debilidad en el sistema que puede permitir que una amenaza se materialice. (Gómez, A. 2011, pg. 61).

Incidente de seguridad

Es un evento que provoca la interrupción de servicios, es la materialización de una amenaza. (Gómez, A. 2011, pg. 62).

Impacto

Es la medición del daño que puede causar un incidente de seguridad. (Gómez, A. 2011, pg. 62).

Riesgo

El riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad y cause un impacto en la organización. (Gómez, A. 2011, pg. 63).

NTE INEN ISO/IEC 27005:2012

Este documento normativo se refiere a la Gestión del Riesgo en la Seguridad de la Información, como un complemento paras las normas 27001 y 27002. (INEN 27005:2012, 2012, pg. 1).

Gestión de Riesgos

Forma parte de la gestión integral de la seguridad de la información y debe ser considerando desde la implementación y a lo largo del ciclo de vida de la gestión de seguridad. (INEN 27005:2012, 2012, pg. 3).

El proceso de gestión del riesgo es un ciclo de acciones que abarca la identificación, valoración, tratamiento, aceptación, comunicación, monitoreo y revisión. (INEN 27005:2012, 2012, pg. 4).

- ***La identificación del riesgo*** es importante para dar soporte a la gestión de la seguridad de la información, la continuidad del negocio, respuesta a incidentes y la identificación de requisitos de seguridad propios de un producto o servicio. (INEN 27005:2012, 2012, pg. 11).
- ***La evaluación del riesgo*** debe permitir identificar las acciones de tratamiento del riesgo, caso contrario se requiere una nueva valoración en la que se puede medir el nivel del grado de aceptación o impacto del riesgo. Los criterios de evaluación están relacionados con el valor de la

información, la criticidad de los activos, la normativa legal, la importancia de la confidencialidad, integridad y disponibilidad. Así, el impacto está relacionado con el nivel de sensibilidad de la información, impacto en la pérdida de la confidencialidad, integridad y disponibilidad, costos de recuperación, imagen institucional, incumplimiento legal. (INEN 27005:2012, 2012, pg. 17).

- ***El tratamiento del riesgo*** se orienta a la definición de controles de seguridad que permitan reducir, retener, evitar o transferir los mismos; acción que depende del resultado de valoración del riesgo, costo operativo y beneficios esperados. (INEN 27005:2012, 2012, pg. 18, 19, 20).
- ***La aceptación del riesgo*** se refiere a la conformidad respecto al tratamiento del riesgo, considerando que en cualquier medida la institución es responsable del impacto del riesgo, y el riesgo residual (riesgo que puede permanecer a pesar de los controles implementados). (INEN 27005:2012, 2012, pg. 21).
- ***La comunicación del riesgo*** se refiere a la coordinación efectiva al interno de la organización que permita unificar criterios respecto a la valoración del riesgo, seguridad en su gestión y herramientas de toma de decisiones. (INEN 27005:2012, 2012, pg. 22).
- ***El monitoreo del riesgo*** es importante considerando que los riesgos no son estáticos y su valoración puede cambiar conforme las vulnerabilidades, amenazas y probabilidad de ocurrencia se alteren, por lo que es preciso una revisión permanente de nuevos activos, reevaluación de riesgos, identificación de nuevas amenazas y vulnerabilidades, cambio en la percepción del impacto e incidentes de
- seguridad sucedidos. (INEN 27005:2012, 2012, pg. 23).
- ***Revisión de la gestión del riesgo*** que permita mejorar de forma constante la identificación, valoración y tratamiento del riesgo, que esta

sea actualizada y acorde a la sensibilidad del activo de información. (INEN 27005:2012, 2012, pg. 24).

Buenas prácticas en seguridad

En general se refieren al empleo de procedimiento sistemáticos que permitan una adecuada gestión de la seguridad. Se basan en la experiencia y estándares aprobados y buscan garantizar la eficiencia en la gestión de la seguridad, la disminución de incidentes de seguridad y la satisfacción de los usuarios.

Sistema de Gestión de Seguridad de la Información (SGSI)

La implantación de un sistema de gestión de seguridad de la información, se desarrolla en las siguientes etapas:

1. Definición del alcance: procesos, procedimientos y recursos considerados para la gestión.

2. Establecimiento de políticas: Definir conforme el alcance planificado, las políticas respecto a todos los procedimientos que involucran el negocio.

3. Documentación: respecto a los principios, responsabilidades, soporte documental, cumplimiento legal.

4. Análisis y Gestión de riesgos: proceso sistemático de definición de activos (recursos software, hardware, humanos, comunicaciones, bases de datos), identificación de vulnerabilidades y amenazas, evaluación del riesgo con base a la probabilidad de ocurrencia y el impacto en el negocio.

Considerando que la Auditoría es la fase que permite identificar el nivel de exposición, es necesario complementar con el análisis de riesgos que facilita su evaluación y recomendaciones con base al análisis costo – beneficio de su aplicación. (Piattini, M. 2008, pg. 58).

Para la gestión de riesgos se considera cuatro posibles escenarios que son:

- Evitarlos: Se refiere a las medidas preventivas que se tomen, respecto a un análisis de posibles ocurrencias.
- Transferirlos: Cuando se transfiere la responsabilidad a un tercero. Podría ser a través de la externalización del servicio de seguridad.
- Reducirlos: Mediante la implantación de políticas de seguridad, su monitoreo y actualización permanente.
- Asumirlos: Se refiere al nivel de riesgo que la entidad está dispuesta a asumir, considerando los costos por pérdida que estos generen. (Piattini, M. 2008, pg. 59).

5. Selección de controles y objetivos de seguridad: Respecto al análisis de disponibilidad económica, de infraestructura, y necesidades del negocio. Se establece el DSC (Documento de selección de controles). (Gómez, A. 2011, pg. 160, 161).

Ciclo de vida de un SGSI

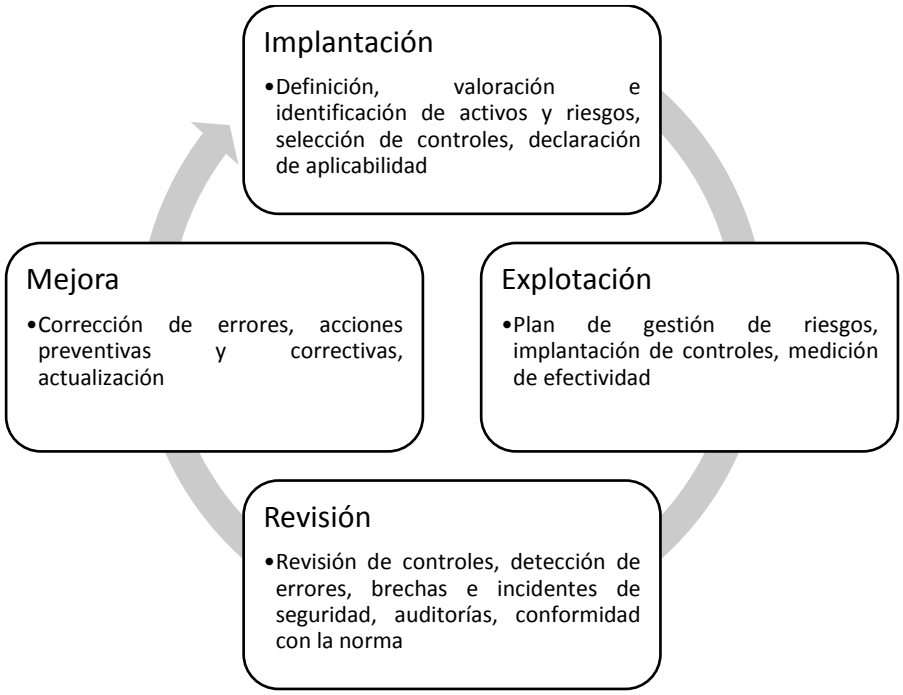


Gráfico 34 Ciclo de vida SGSI
Fuente: Àlvaro Gómez Vieites, 2011, pg 162, 163
Elaborado por: La Investigadora

Tipos de información

Para una adecuada gestión de la información es importante realizar la clasificación de la misma, conforme su nivel de sensibilidad y confidencialidad, así:

- Información sin clasificar o desclasificada. – De conocimiento público.
- Información de uso interno. – Para gestión interna institucional. No necesita ser divulgada a terceros.
- Información confidencial. – Para acceso y uso por un determinado grupo de personas. Su acceso no autorizado puede ocasionar perjuicios o inconvenientes a la entidad.

- Información secreta o reservada. – De carácter estratégico, solo para nivel directivo. Su divulgación puede ocasionar graves daños a la organización. (Gómez, A. 2011, pg. 112)

Posicionamiento estratégico

Es la representación gráfica de la situación actual de una institución, que evalúa el desempeño de sus componentes y permite establecer el nivel de esfuerzo que deberá ser empleado en su mejora respecto a la importancia de estos. (MAPCAL, 1990, pg.7)

Para Bruneer (2008), citado por Bionel, A. 2013. pg. 17, la matriz de posicionamiento permite a una IES determinar que producto o servicio debe mejorarse.

6.7 Metodología, Modelo operativo

Para la gestión de seguridad se toma como base las referencias de las normas NTE INEN ISO/IEC 27001:2013 y 27005:2012 respecto a la seguridad de la información y la gestión de riesgos.

Conforme los resultados de la auditoría aplicada, el proceso para la gestión de la seguridad se enmarca dentro del siguiente esquema:

1. Identificar y evaluar los activos de información para establecer los requisitos de seguridad propios de cada uno.

2. Análisis estratégico de posicionamiento (madurez vs importancia) de los controles de seguridad evaluados en la UNACH, que permita establecer la prioridad de gestión respecto a la seguridad de la información.

3. Lo antes citado permitirá determinar las acciones jerárquicamente prioritarias que deba implementar la institución, dentro de la gestión en seguridad.

1. Identificación y evaluación de activos de información

1.1. Definición y alcance

a. Objetivo:

- Identificar y evaluar los riesgos respecto a los activos de información como parte del plan de respuesta a incidentes y continuidad del negocio (gestión de seguridad), para la Unidad Técnica de Control Académico de la UNACH.

b. Misión de la Unidad Técnica de Control Académico:

- Desarrollar aplicaciones informáticas para ejercer el control académico estudiantil.
- Desarrollar aplicaciones informáticas que permitan administrar los servicios proporcionados por la institución en el campo académico.
- Implementar servicios académicos para estudiantes y docentes a través de internet.

- Capacitar a los funcionarios universitarios, en el uso correcto de las aplicaciones informáticas desarrolladas por esta unidad.
- Brindar el soporte y logística en cuanto al sistema académico se refiere, cuando sea necesario.
- Proporcionar información académica a los diferentes departamentos que lo requieran para la toma de decisiones. (Reglamento UTECA (no aprobado), pg. 3).

b. Normativa Legal que la rige

- Ley Orgánica de Educación Superior
- Estatuto de la Universidad Nacional de Chimborazo
- Reglamento de Régimen Académico
- Toda ley, norma o decreto que se aplique a la institución y su área de injerencia sea la gestión académica

c. Restricciones

- Preexistente:
    - La Unidad Técnica de Control Académico se encuentra en proceso de reestructuración y fusión con el Centro de Tecnología Educativa en adaptación al nuevo modelo por procesos que está implementando la institución, por lo que la propuesta se enmarca a la operación actual de dicha unidad.
    - Una vez que la nueva estructura se encuentre aprobada, se deberá adaptar la gestión del riesgo al contexto global del nuevo proceso.

- Técnicas:
    - La arquitectura, infraestructura y redes de comunicación que establece el área de Administración de Redes.
    - Los sistemas operativos y paquetes de software propietario que cuentan licencia y que han sido adquiridos por el Centro de Tecnología Educativa.

- Físicas:
    - La edificación y cumplimiento de normativa legal para construcción, instalaciones eléctricas, hidrosanitarias, del cuerpo de bomberos, de riesgos y seguridad laboral, y demás que relacionadas al permiso y habilitación de un espacio físico.

- Económicas:
    - Conforme el presupuesto que sea priorizado por la institución para el área y la gestión de seguridad.

- Tiempo:
    - Previsión de ejecución en un plazo de 6 meses.

- Organizacionales:
    - Recursos humanos con los que cuenta el área y que puedan ser asignados para complementar el proceso.
    - Responsabilidades de la unidad.

1.2 Identificación de activos

En la identificación y valoración de riesgos de los activos de información, participaron los 3 funcionarios que laboran en la Unidad Técnica de Control Académico (Coordinador, Administrador de Bases de Datos, Desarrollador de Software)

Tabla 9 Activos de Información - UTECA - UNACH

No	Activos Primarios	Activos de soporte
1	Información personal de estudiantes, docentes, administrativos y trabajadores.	Servidor de Bases de Datos
2	Información académica (inscripciones, matriculación, calificaciones, egresamiento, graduación).	Servidor de Aplicaciones
3	Información estratégica (socioeconómica, estadística, indicadores de impacto, resultado y gestión)	Equipos – Estaciones de trabajo
4	Información documental (respecto a los procesos internos	Equipos portátiles de cómputo
5		Tabletas electrónicas
6		Impresoras
7		Discos externos, CD, DVD, etc.
8		Sistemas Operativos
9		Software para administración de bases de datos
10		Software para servidor web
11		Sistemas
12		Código fuente
13		Red de comunicaciones (pública y local)
14		Personal (directivos, técnicos, usuarios)
15		Instalaciones (edificio, oficinas, centro de datos,
16		Estructura (organización interna, proyectos, proveedores)

Fuente: Unidad Técnica de Control Académico
Elaborado por: La Investigadora

1.3 Valoración de activos

La valoración de los activos se realiza utilizando una escala cuali-cuantitativa en función del impacto que ocasionaría la pérdida de las características

fundamentales de la información como son: confidencialidad, integridad y disponibilidad, conforme se observa en la siguiente tabla:

Tabla 10 Escala de valoración del activo respecto al impacto

Valoración	Confidencialidad	Integridad	Disponibilidad
1	**Bajo:** La información puede ser difundida sin restricciones, sin que esto ocasione conflictos al giro del negocio. Acceso y/o divulgación de información interna no publicada.	**Bajo:** La pérdida de precisión de la información no genera afectación a la institución y su imagen. Pérdida menor de recursos	**Bajo:** Si hay problemas en la disponibilidad de información, no se ve afectada la operación normal de los procesos asociados. Disminución en el rendimiento
2	**Moderado:** Esta información puede ser utilizada por los integrantes de la entidad, pero no puede ser divulgada sin autorización. Acceso y/o divulgación de información confidencial	**Moderado:** La pérdida de precisión de la información genera un impacto negativo moderado en la operación normal de la institución y su imagen. Pérdida de recursos críticos, de los cuales se tiene respaldo	**Moderado:** Si hay problemas en la disponibilidad de información, existe una afectación moderada a la operación normal de los procesos asociados. Notable disminución de rendimiento
3	**Alto:** La información se puede utilizar solo para procedimientos específicos de la organización. Su divulgación puede generar problemas legales, pérdidas, impacto negativo en la imagen institucional. Acceso y/o divulgación de información estratégica o protegida	**Alto:** La pérdida de precisión de la información genera un impacto negativo alto en la operación normal de la institución y su imagen. Pérdida grave de recursos, no recuperable o a un costo muy alto. Pérdida de credibilidad en el sistema de información.	**Alto:** Si hay problemas en la disponibilidad de información, existe una afectación severa a la operación normal de los procesos asociados. Paralización de procesos.

Elaborado por: La Investigadora

1.4 Identificación de amenazas

Permite determinar el peligro al que pueden estar expuestos los activos de información y se los ha agrupado por su tipología en factor humano, de software y de hardware, así:

Tabla 11 Identificación de amenazas

Tipo	Amenazas	Descripción
	Negligencia	Uso irresponsable de la información, los equipos o claves de acceso. Incluye no considerar los respaldos de información.
	Ingeniería social	Obtener información confidencial a través de la manipulación a los usuarios.
	Falta de personal	Personal insuficiente para cumplir responsabilidades de la unidad
	Intrusos	Intrusos con conocimientos informáticos con el deseo de explotar vulnerabilidades con o sin la intención de hacer daño.
	Uso de no autorización de información. Espionaje	Uso o divulgación de información institucional sin autorización
	Malware (Virus, troyanos, gusanos, spyware, etc.)	Cualquier software con la intención de alterar, dañar u obtener información sin autorización.
	Capacidad del sistema	Soporte a conexiones multiusuario
	Bug de sistema	Error o fallo de software
	Falsificación de derechos	Gestión ineficiente de privilegios de acceso
	Software propietario sin licencia	Instalación y uso de software propietario sin licencia
	Robo /hurto de equipos	Pérdida total de equipos por robo o hurto
	Desastres naturales	Inundaciones, terremotos, tormentas, etc.
	Daño del equipos o sus partes	Desactualización, sobrecalentamiento o equipos quemados que puedan comprometer la seguridad de la información
	Red de comunicaciones	Falla en los equipos de telecomunicaciones, interceptación de señales, escasos protocolos de seguridad, inadecuada gestión de la red, etc.

Fuente: Unidad Técnica de Control Académico
Elaborado por: La Investigadora

1.5 Valoración del riesgo

Para realizar la valoración del riesgo se considera el método de asociación entre el valor del activo, la amenaza y la probabilidad de ocurrencia.

La probabilidad de ocurrencia de la amenaza se valora conforme la siguiente escala:

Tabla 12 Escala de valoración de la probabilidad de ocurrencia de la amenaza

Valoración	Escala cualitativa	Descripción
1	Baja	Las condiciones y esfuerzos institucionales hacen que sea muy baja la posibilidad de ocurrencia de la amenaza
2	Moderada	Las condiciones y esfuerzos institucionales evidencian una moderada probabilidad de ocurrencia de la amenaza
3	Alta	Las condiciones y esfuerzos institucionales evidencian un alta o inminente probabilidad de ocurrencia de la amenaza

Elaborado por: La Investigadora

Para determinar la valoración del riesgo se utiliza la siguiente fórmula:

Riesgo = Promedio del valor del activo multiplicado por la probabilidad de ocurrencia de la amenaza.

Sus resultados se interpretan así:

Tabla 13 Valoración del riesgo

No	Rango	Descripción	Tipo de Riesgo semaforización
1	0 - 3	Riesgo aceptable. Se puede retener.	**Bajo**
2	4 – 6	Riesgo que necesita prevención. Reducción del riesgo	**Moderado**
3	7 - 9	Riesgo que necesita mitigación. Reducción, transferencia o evitación del riesgo.	**Alto**

Elaborado por: La Investigadora

De la identificación y evaluación de riesgos respecto a los activos de información de la Unidad Técnica de Control Académico, se obtienen los siguientes resultados:

Institución: **UNIVERSIDAD NACIONAL DE CHIMBORAZO**

Departamento: **Unidad Técnica de Control Académico**

Tabla 14 Matriz de identificación y evaluación de riesgos de seguridad de la información

No	Tipo de activo	Activo de Información	Tipo de amenaza	Amenaza	Probabilidad de ocurrencia	Impacto - Valor del activo			Evaluación del riesgo
						Confidencialidad	Integridad	Disponibilidad	
1	primario	Información personal Información académica Información estratégica	Factor Humano	Ingeniería Social	2	3	3	3	6
2	primario	Información personal Información académica Información estratégica	Factor Humano	Negligencia	1	3	3	3	3
3	primario	Información personal Información académica Información estratégica	Factor Humano	Intrusos	2	3	3	3	6
4	primario	Información personal Información académica Información estratégica	Factor Humano	Uso no autorizado de información. Espionaje	2	3	3	3	6
5	primario	Información personal Información académica Información estratégica	Software	Falsificación de derechos	1	3	3	3	3
6	primario	Información personal Información académica Información estratégica	Software	Capacidad del sistema	1	3	3	3	3
7	primario	Información personal Información académica Información estratégica	Hardware	Red de comunicaciones	1	3	3	3	3
8	primario	Información personal Información académica Información estratégica	Hardware	Daño del equipo o sus partes	1	3	3	3	3

No	Tipo de activo	Activo de Información	Tipo de amenaza	Amenaza	Probabilidad de ocurrencia	Impacto - Valor del activo			Evaluación del riesgo
						Confidencialidad	Integridad	Disponibilidad	
9	soporte	Servidor de Base de Datos	Factor Humano	Negligencia	1	3	3	3	3
10	soporte	Servidor de Base de Datos	Factor Humano	Intrusos	1	3	3	3	3
11	soporte	Servidor de Base de Datos	Software	Capacidad del sistema	2	3	3	3	6
12	soporte	Servidor de Base de Datos	Software	Falsificación de derechos	1	3	3	3	3
13	soporte	Servidor de Base de Datos	Hardware	Daño del equipo o sus partes	1	3	3	3	3
14	soporte	Servidor de Base de Datos	Hardware	Red de comunicaciones	2	3	3	3	6
15	soporte	Servidor de Aplicaciones	Factor Humano	Intrusos	2	3	3	3	6
16	soporte	Servidor de Aplicaciones	Factor Humano	Negligencia	1	3	3	3	3
17	soporte	Servidor de Aplicaciones	Software	Malware	2	1	2	3	4
18	soporte	Servidor de Aplicaciones	Software	Bug de sistema	1	3	3	3	3
19	soporte	Servidor de Aplicaciones	Hardware	Daño del equipo o sus partes	1	1	1	3	2
20	soporte	Servidor de Aplicaciones	Hardware	Red de comunicaciones	2	3	3	3	6
21	soporte	Código fuente	Humano	Uso no autorizado	1	1	1	1	1
22	soporte	Código fuente	Software	Falsificación de derechos	1	1	1	1	1
23	soporte	estaciones de trabajo equipos portátiles	Factor Humano	negligencia	1	3	3	3	3
24	soporte	estaciones de trabajo equipos portátiles	Factor Humano	Uso no autorizado de información. Espionaje	1	3	3	3	3

No	Tipo de activo	Activo de Información	Tipo de amenaza	Amenaza	Probabilidad de ocurrencia	Impacto - Valor del activo			Evaluación del riesgo
						Confidencialidad	Integridad	Disponibilidad	
25	soporte	estaciones de trabajo equipos portátiles	Software	malware	1	3	3	3	3
26	soporte	estaciones de trabajo equipos portátiles	Hardware	Robo/ hurto de equipos	1	3	3	3	3
27	soporte	estaciones de trabajo equipos portátiles	Hardware	Daño del equipo o sus partes	1	3	3	3	3
28	soporte	impresoras	Hardware	Red de comunicaciones	2	3	1	1	3
29	soporte	Unidades de almacenamiento externo	Factor Humano	negligencia	1	3	3	3	3
30	soporte	Unidades de almacenamiento externo	Software	malware	2	3	3	3	6
31	soporte	Unidades de almacenamiento externo	Hardware	Robo/ hurto de equipos	2	3	3	3	6
32	soporte	Unidades de almacenamiento externo	Hardware	Daño del equipo o sus partes	2	3	3	3	6
33	soporte	Sistemas Operativos	Factor Humano	negligencia	1	1	2	3	2
34	soporte	Sistemas Operativos	Software	malware	1	3	1	3	2
35	soporte	Sistemas Operativos	Software	Software propietario sin licencia	1	1	3	3	2
36	soporte	Software para administración de base de datos Software para servidor web	Factor Humano	negligencia	1	3	3	3	3
37	soporte	Software para administración de base de datos Software para servidor web	Factor Humano	intrusos	1	3	3	3	3
38	soporte	Software para administración de base de datos Software para servidor web	Software	Capacidad del sistema	1	3	3	3	3

No	Tipo de activo	Activo de Información	Tipo de amenaza	Amenaza	Probabilidad de ocurrencia	Impacto - Valor del activo			Evaluación del riesgo
						Confidencialidad	Integridad	Disponibilidad	
39	soporte	Software para administración de base de datos Software para servidor web	Software	Falsificación de derechos	1	3	3	3	3
40	soporte	Software para administración de base de datos Software para servidor web	Hardware	Red de comunicaciones	2	3	3	3	6
41	soporte	Sistemas	Factor Humano	negligencia	1	3	3	3	3
42	soporte	Sistemas	Factor Humano	Falta de personal	2	3	2	1	4
43	soporte	Sistemas	Software	Bug de sistema	1	1	1	3	2
44	soporte	Sistemas	Hardware	Daño del equipo o sus partes	1	1	1	3	2
45	soporte	Sistemas	Hardware	Red de comunicaciones	2	3	3	3	6
46	soporte	Red de comunicaciones	Factor Humano	Falta de personal	2	2	2	3	5
47	soporte	Red de comunicaciones	Factor Humano	intrusos	2	3	3	3	6
48	soporte	Red de comunicaciones	Factor Humano	negligencia	1	3	3	3	3
49	soporte	Red de comunicaciones	Software	Capacidad del sistema	2	2	2	3	5
50	soporte	Red de comunicaciones	Software	Falsificación de derechos	2	3	3	3	6
51	soporte	Red de comunicaciones	Hardware	Desastres naturales	1	1	1	3	2
52	soporte	Red de comunicaciones	Hardware	Daño del equipo o sus partes	1	1	1	3	2
53	soporte	Personal	Factor Humano	Ingeniería Social	2	3	3	3	6
54	soporte	Personal	Factor Humano	Uso no autorizado de información. Espionaje	2	3	3	3	6

No	Tipo de activo	Activo de Información	Tipo de amenaza	Amenaza	Probabilidad de ocurrencia	Impacto - Valor del activo			Evaluación del riesgo
						Confidencialidad	Integridad	Disponibilidad	
55	soporte	Personal	Factor Humano	negligencia	2	3	3	3	6
56	soporte	Instalaciones	Factor Humano	negligencia	1	3	2	3	3
57	soporte	Instalaciones	Factor Humano	Falta de personal	1	2	2	2	2
58	soporte	Instalaciones	Software	Falsificación de derechos	1	3	3	3	3
59	soporte	Estructura - proyectos	Software	Bug de sistema	1	3	3	3	3
60	soporte	Estructura - proyectos	Factor Humano	negligencia	1	3	3	3	3

Fuente: Unidad Técnica de Control Académico

Elaborado por: La Investigadora

Riesgos con baja probabilidad de ocurrencia:	39
Riesgos con moderada probabilidad de ocurrencia:	21
Riesgos con alta probabilidad de ocurrencia:	0
TOTAL	60

De la valoración realizada se puede observar que:

- El 65% de los riesgos tienen una probabilidad baja de ocurrencia (negligencia en el uso de información, capacidad del sistema, falsificación de derechos, daño de equipos, malware), el riesgo es aceptable, por lo que no se requiere implementar controles adicionales. Se puede retener.
- El 35% de los riesgos tienen una probabilidad moderada de ocurrencia (ingeniería social, intrusos, red de comunicaciones falta de personal), por lo que es necesario se seleccione e implemente los controles adecuados, que permita corregir, prevenir o minimizar el impacto; sobre cuyo resultado se deberá reevaluar el riesgo hasta llegar al nivel de aceptación. El riesgo se debe reducir.
- Ningún riesgo tiene alta probabilidad de ocurrencia.

2. *Análisis estratégico de posicionamiento (madurez vs importancia) de los controles de seguridad en la Unidad Técnica de Control Académico*

El análisis estratégico de posicionamiento de los controles de seguridad se realiza con la finalidad de determinar el nivel de desempeño (madurez alcanzada) respecto a la importancia del control, a fin de poder clasificarlos de acuerdo a la prioridad de implementación, tratamiento y mejora.

Para esto se ha establecido una matriz bidimensional de posicionamiento del control, bajo los siguientes parámetros así:

Tabla 15 Matriz de posicionamiento del control de seguridad

Criticidad	Rango de operación	Interpretación
I	Nivel de madurez Bajo o Medio e Importancia Alta o Vital	Priorizar atención. Los controles no cumplen las garantías de seguridad esperadas. Requiere plan de intervención
II	Nivel de madurez Alto o Excelente e Importancia Alta o Vital	Mantener desempeño. Se debe documentar el procedimiento y/o política. Los controles cumplen garantías adecuadas de seguridad. Requiere monitoreo
III	Nivel de madurez Bajo o Medio e Importancia Baja o Media	Baja prioridad. Los controles no son necesarios para los procesos, su aporte es secundario o se cuenta con otro mecanismo de seguridad. No requiere atención.
IV	Nivel de madurez Alto o excelente e Importancia Baja o Media	Exceso de esfuerzos. Los esfuerzos respecto al control son innecesarios de acuerdo al aporte de seguridad que genera. Requiere disminuir atención

Elaborado por: La Investigadora

El análisis estratégico de posicionamiento con base a los parámetros antes citados, arrojan los siguientes resultados:

Tabla 16 Resultado estratégico posicionamiento de controles de seguridad

No	Objetivo de control Norma 27001	Control	Nivel de Madurez	Importancia	Posicio-namiento
1		5.1.1 Política de seguridad de la información para los SGBD	Medio	Alta	I
2		5.1.2 Revisiones a la política de seguridad	Medio	Alta	I
3		6.1.1 Roles y responsabilidades de seguridad de la información	Medio	Alta	I
4		6.1.2 Separación de funciones	Medio	Vital	I
5		6.1.3 Contacto con las autoridades	Medio	Media	I
6		6.1.4 Contacto con grupos de interés especial	Alto	Alta	II
7		6.1.5 Gestión de Proyecto de seguridad de la información	Medio	Vital	I
8		6.2.1 Política de dispositivo móvil	Medio	Alta	I
9		6.2.2 Teletrabajo	Alto	Alta	II
10		7.1.1 Investigación de antecedentes	Alto	Alta	II
11		7.1.2 Términos y condiciones laborales	Medio	Vital	I
12		7.2.1 Responsabilidades de la Dirección	Medio	Alta	I
13		7.2.2 Concienciación, educación y formación en seguridad de la información	Bajo	Alta	I
14		7.2.3 Proceso disciplinario	Bajo	Alta	I
15		7.3.1 Responsabilidad por finalización o cambio de empleo	Medio	Vital	I
16		8.1.1 Inventario de activos	Bajo	Vital	I
17		8.1.2 Propiedad de los activos	Medio	Alta	I
18		8.1.3 Uso aceptable de los activos	Medio	Alta	I
19		8.1.4 Devolución de activos	Medio	Alta	I
20		8.2.1 Clasificación de la información	Bajo	Alta	I
21		8.2.2 Etiquetado de la información	Bajo	Media	I
22		8.2.3 Manejo de activos	Alto	Alta	II
23		8.3.1 Gestión y transferencia de medios extraíbles	Medio	Alta	I
24		8.3.2 Eliminación de los medios	Medio	Alta	I
25		8.3.3 Transferencia de medios físicos	Medio	Vital	I
26		9.1.1 Política de control de acceso	Medio	Alta	I
27		9.1.2 Acceso a redes y servicios de red	Medio	Alta	I
28		9.2.1 Registro y retiro de usuarios	Medio	Alta	I
29		9.2.2 Provisión de accesos a usuarios	Medio	Alta	I
30		9.2.3 Gestión de privilegios de derechos de acceso	Alto	Alta	II
31		9.2.4 Gestión de la información secreta de autenticación de los usuarios	Alto	Alta	II
32		9.2.5 Revisión de los derechos de acceso de usuarios	Medio	Alta	I
33		9.2.6 Retiro y ajuste de los derechos de acceso	Alto	Alta	II
34		9.3.1 Uso de información secreta de autenticación	Medio	Alta	I
35		9.4.1 Restricción del acceso a la información	Alto	Vital	II
36		9.4.2 Procedimientos seguros de inicio de sesión	Alto	Alta	II
37		9.4.3 Sistema de gestión de contraseñas	Alto	Alta	II

No	Objetivo de control Norma 27001	Control	Nivel de Madurez	Importancia	Posicio-namiento
38		9.4.4 Uso de programas utilitarios privilegiados	Alto	Alta	II
39		9.4.5 Control de acceso al código fuente del programa	Alto	Vital	II
40		10.1.1 Política de uso de los controles criptográficos	Medio	Alta	I
41		10.1.2 Gestión de llaves	Medio	Media	II
42		11.1.1 Perímetro de seguridad física	Alto	Vital	II
43		11.1.2 Controles físicos de entrada	Alto	Vital	II
44		11.1.3 Seguridad de oficinas, despachos e instalaciones	Alto	Alta	II
45		11.1.1 Protección contra las amenazas externas y ambientales	Alto	Vital	II
46		11.1.5 Trabajo en áreas seguras	Medio	Vital	I
47		11.1.6 Áreas de carga y entrega	Alto	Vital	II
48		11.2.1 Ubicación y protección de equipos	Alto	Vital	II
49		11.2.2 Instalaciones de suministro	Alto	Vital	II
50		11.2.3 Seguridad del cableado	Alto	Vital	II
51		11.2.4 Mantenimiento de los equipos	Alto	Vital	II
52		11.2.5 Eliminación de activos	Bajo	Alta	I
53		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	Medio	Alta	I
54		11.2.7 Reutilización o eliminación segura de equipos	Alto	Alta	II
55		11.2.8. Equipos de usuario desatendido	Medio	Vital	I
56		11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Alto	Alta	II
57		12.1.1 Documentación de procedimientos de operación	Medio	Alta	I
58		12.1.2 Gestión de cambios	Medio	Vital	I
59		12.1.3 Gestión de capacidades	Medio	Alta	I
60		12.1.4 Separación de ambientes de desarrollo, pruebas y producción	Alto	Alta	II
61		12.2.1 Controles contra malware	Alto	Alta	II
62		12.3.1 Copias de seguridad de la información	Medio	Vital	I
63		12.4.1 Registro de eventos	Medio	Vital	I
64		12.4.2 Protección de la información de registro	Medio	Vital	I
65		12.4.3 Registros de administración y operación	Medio	Vital	I
66		12.4.4 Sincronización del reloj	Alto	Alta	II
67		12.5.1 Instalación del software en los sistemas operativos	Alto	Alta	II
68		12.6.1 Gestión de las vulnerabilidades técnicas	Medio	Vital	I
69		12.6.2 Restricciones en la instalación del software	Alto	Alta	II
70		12.7.1 Controles de auditoría de sistemas de información	Alto	Alta	II
71		13.1.1 Controles de red	Alto	Vital	II
72		13.1.2 Seguridad de los servicios de red	Alto	Alta	II
73		13.1.3 Separación en las redes	Alto	Alta	II

No	Objetivo de control Norma 27001	Control	Nivel de Madurez	Importancia	Posicio-namiento
74		13.2.1 Políticas y procedimientos de transferencia de información	Medio	Media	I
75		13.2.2 Acuerdos de transferencia de información	Alto	Alta	II
76		13.2.3 Mensajería electrónica	Bajo	Alta	I
77		13.2.4 Acuerdos de confidencialidad o no revelación	Medio	Alta	I
78		14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Alto	Vital	II
79		14.1.2 Asegurar los servicios de aplicaciones en redes públicas	Alto	Vital	II
80		14.1.3 Protección de las transacciones de servicios de aplicaciones	Alto	Vital	II
81		14.2.1 Política de desarrollo seguro	Alto	Vital	II
82		14.2.2 Procedimientos de control de cambios en sistemas	Alto	Alta	II
83		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Alto	Alta	II
84		14.2.4 Restricciones a los cambios en los paquetes de software	Alto	Alta	II
85		14.2.5 Principios de ingeniería de sistemas seguros	Alto	Alta	II
86		14.2.6 Ambiente de desarrollo seguro	Alto	Alta	II
87		14.2.7 Desarrollo externalizado	Medio	Alta	I
88		14.2.8 Pruebas de seguridad del sistema	Alto	Alta	II
89		14.2.9 Pruebas de aceptación de sistemas	Alto	Alta	II
90		14.3.1 Protección de los datos de prueba	Alto	Alta	II
91		15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Medio	Alta	I
92		15.1.2 Requisitos de seguridad en contratos con terceros	Medio	Alta	I
93		15.1.3 Cadena de suministro de tecnologías de la información y de las comunicaciones	Medio	Media	I
94		15.2.1 Monitoreo y revisión de los servicios de proveedores	Medio	Alta	I
95		15.2.2 Gestión de cambios en los servicios de proveedores	Medio	Alta	I
96		16.1.1 Responsabilidades y procedimientos	Medio	Vital	I
97		16.1.2 Informe de los eventos de seguridad de la información	Medio	Vital	I
98		16.1.3 Informe de debilidades de seguridad de la información	Bajo	Alta	I
99		16.1.4 Apreciación y decisión sobre los eventos de seguridad de la información	Medio	Media	I
100		16.1.5 Respuesta a incidentes de seguridad de la información	Medio	Alta	I
101		16.1.6 Aprendizaje de los incidentes de seguridad de la información	Medio	Vital	I
102		16.1.7 Recopilación de evidencias	Medio	Alta	I

No	Objetivo de control Norma 27001	Control	Nivel de Madurez	Importancia	Posicio-namiento
103 104 105	A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	17.1.1 Planificación de la continuidad de seguridad de la información 17.1.2 Implementación de la continuidad de seguridad de la información 17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información	Alto	Alta	II
106		17.2.1 Disponibilidad de las instalaciones de procesamiento de la información	Alto	Alta	II
107		18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Alto	Vital	II
108		18.1.2 Derechos de propiedad intelectual	Alto	Vital	II
109		18.1.3 Protección de los registros	Bajo	Alta	I
110		18.1.4 Protección y privacidad de la información de carácter personal	Medio	Vital	I
111		18.1.5 Reglamentos de controles criptográficos	Alto	Alta	II
112		18.2.1 Revisión independiente de seguridad de la información	Bajo	Vital	I
113		18.2.2 Cumplimiento de las políticas y normas de seguridad	Bajo	Vital	I
114		18.2.3 Comprobación del cumplimiento técnico	Medio	Alta	I

Fuente: Auditoría de seguridad de la información UNACH - Matriz de evaluación nivel de madurez de los controles de seguridad

Elaborado por: La Investigadora

Controles con nivel de madurez inexistente o bajo e importancia alta o vital	61
Controles con nivel de madurez alto o excelente e importancia alta o vital	51
Controles con nivel de madurez inexiste o bajo e importancia baja o media	0
Controles con nivel de madurez alto o excelente e importancia baja o media	0
Total de Controles Valorados	114

Del posicionamiento realizado se puede observar que:

- El 53,51% de controles no cumplen las garantías de seguridad requeridas. Se debe priorizar su atención mediante un plan de intervención.

- El 44,74% de controles cumplen garantías adecuadas de seguridad. Falta documentar el proceso. Se debe mantener el desempeño.
- Ningún control ha sido posicionado como de prioridad baja.
- Ningún control ha sido posicionado como innecesario.

Para un mejor análisis, las siguientes ilustraciones permiten ver el posicionamiento de los controles por objetivo de seguridad:

Gráfico 35 Posicionamiento controles Objetivo A5
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Los dos controles del objetivo A5 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

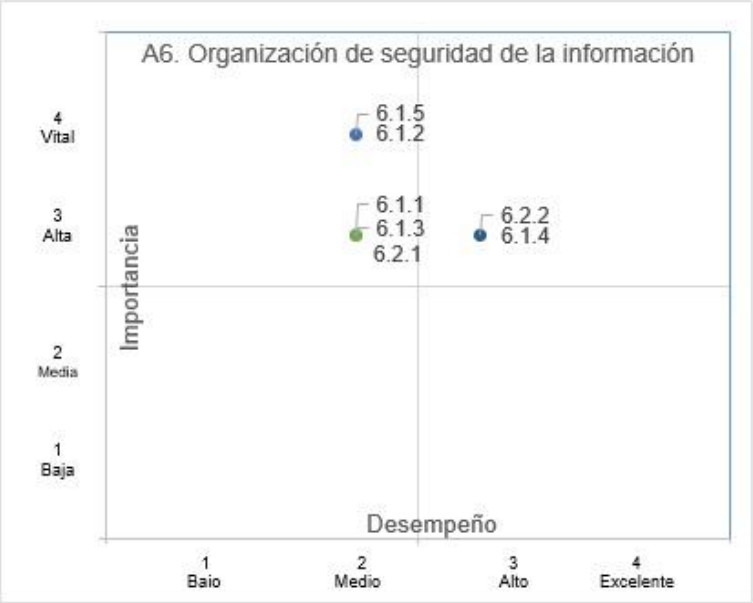


Gráfico 36 Posicionamiento controles Objetivo A6
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Cinco controles del objetivo A6 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de Intervención.

- Dos controles tienen desempeño alto o excelente e importancia alta o vital.
    - Acción: Mantener desempeño. Documentar el proceso.

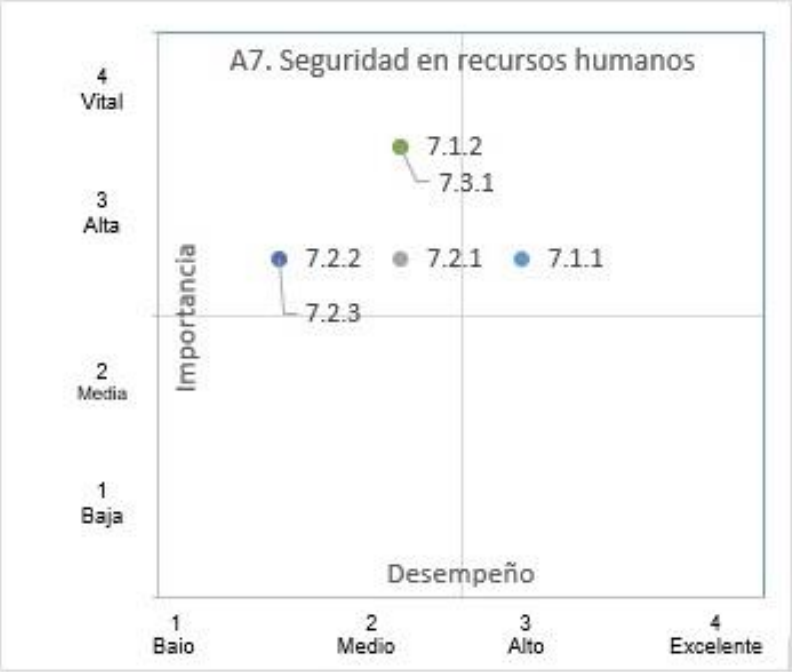


Gráfico 37 Posicionamiento controles objetivo A7
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Cinco controles del objetivo A7 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención.

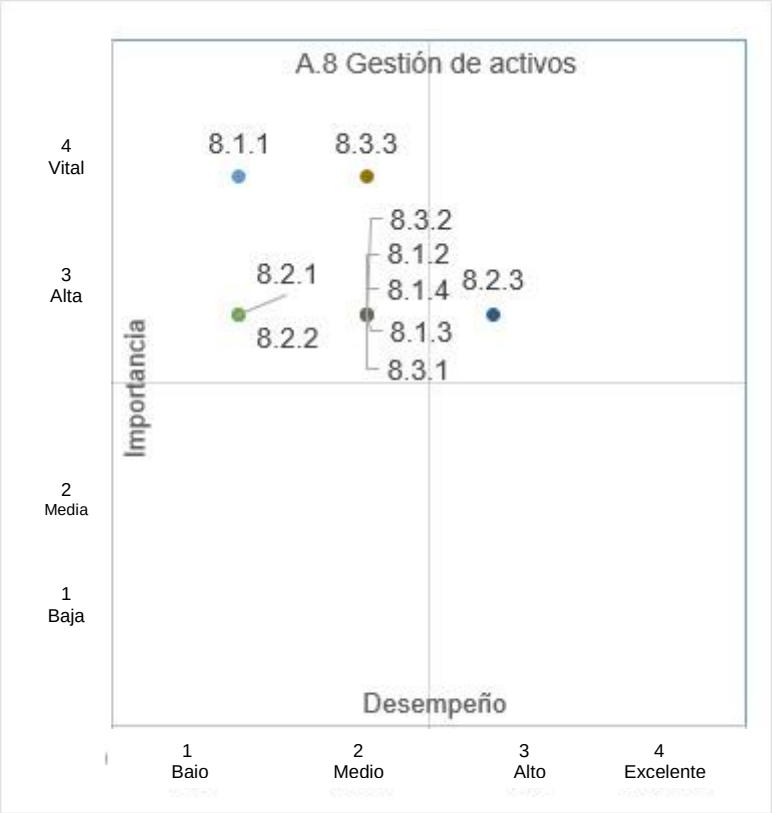


Gráfico 38 Posicionamiento controles objetivo A8
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Nueve controles del objetivo A8 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención.

- Un control tiene desempeño alto o excelente e importancia alta o vital.
    - Acción: Mantener desempeño. Documentar el proceso.

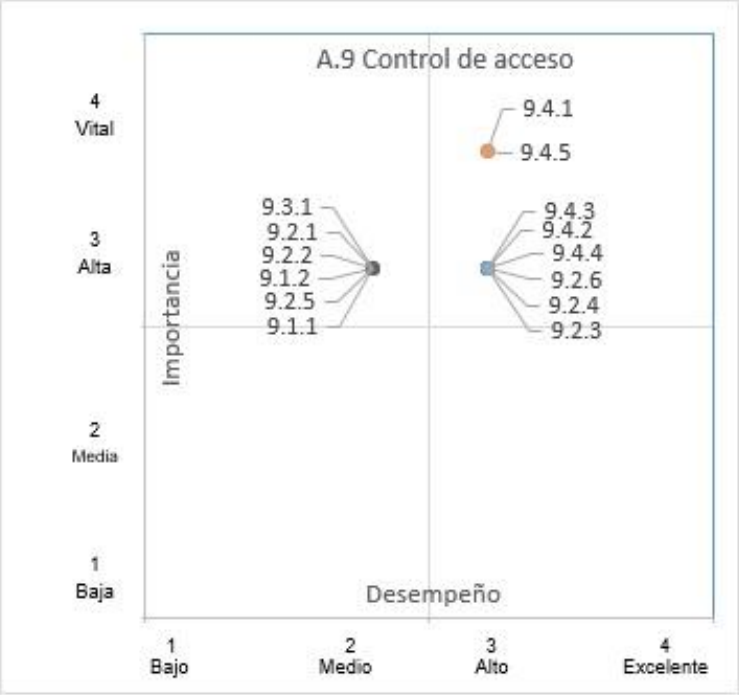


Gráfico 39 Posicionamiento controles objetivo A9
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Seis controles del objetivo A9 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

- Ocho controles tienen desempeño alto o excelente e importancia alta o vital.
    - Acción: Mantener desempeño. Documentar el proceso.

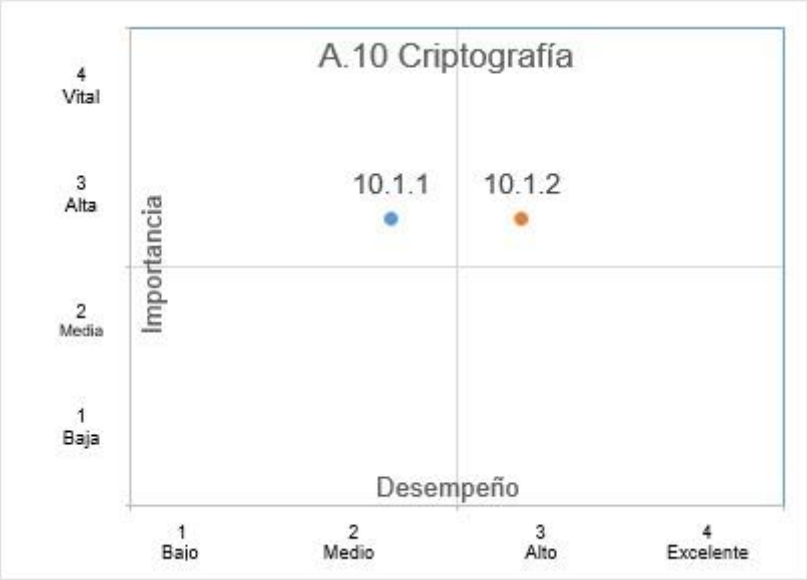


Gráfico 40 Posicionamiento controles objetivo A10
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Un control del objetivo A10 tiene desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

- Un control tiene desempeño alto o excelente e importancia alta o vital.

  Acción: Mantener desempeño. Documentar el proceso.

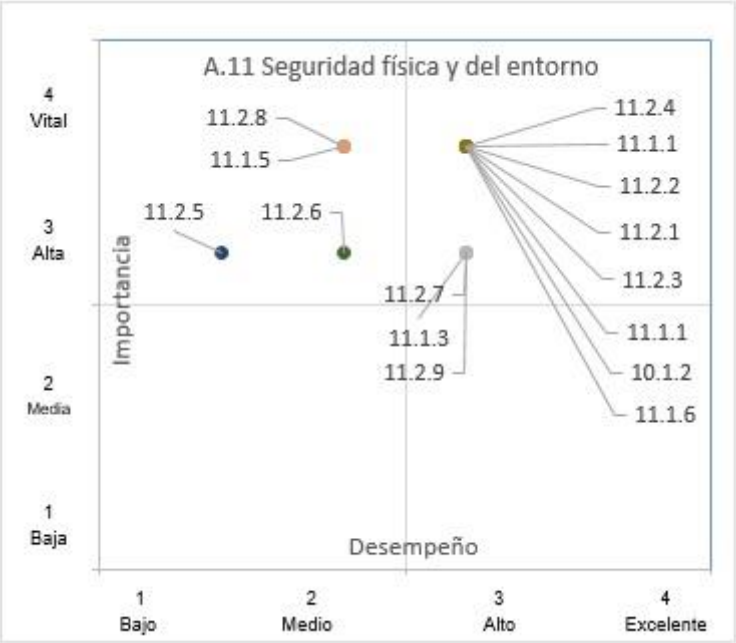


Gráfico 41 Posicionamiento controles objetivo A11
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Cuatro controles del objetivo A11 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

- Once controles tienen desempeño alto o excelente e importancia alta o vital.

    Acción: Mantener desempeño. Documentar el proceso.

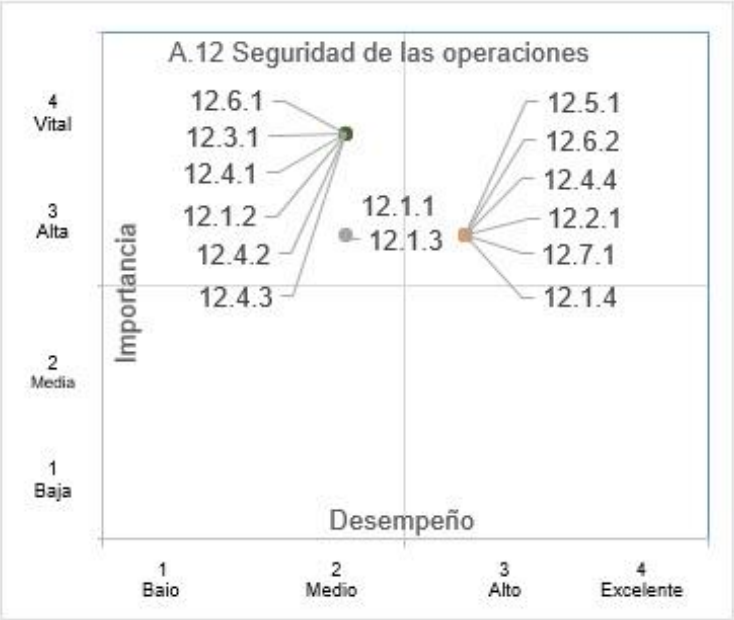


Gráfico 42 Posicionamiento controles objetivo A12
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Ocho controles del objetivo A12 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

- Seis controles tienen desempeño alto o excelente e importancia alta o vital.

    Acción: Mantener desempeño. Documentar el proceso.

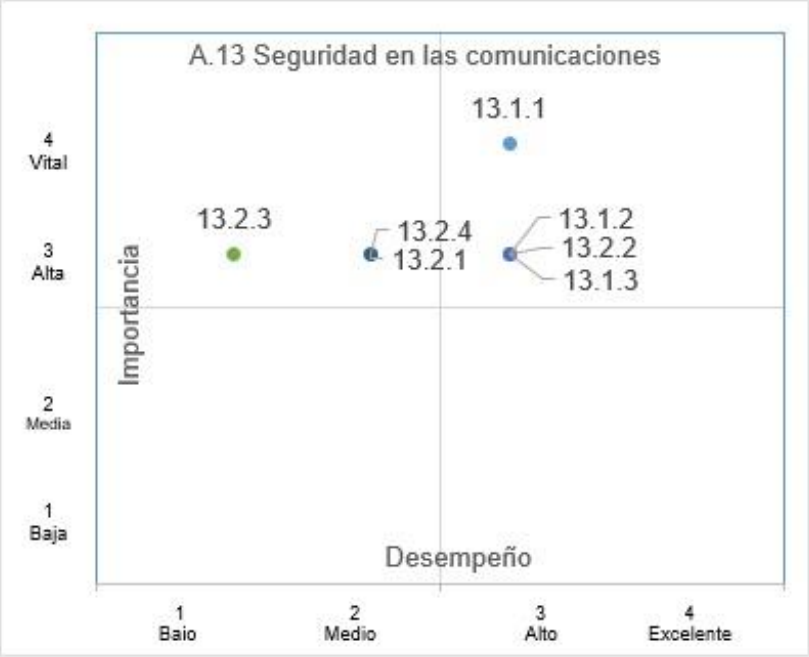


Gráfico 43 Posicionamiento controles objetivo A13
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Tres controles del objetivo A13 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

- Cuatro controles tienen desempeño alto o excelente e importancia alta o vital.
    - Acción: Mantener desempeño. Documentar el proceso.

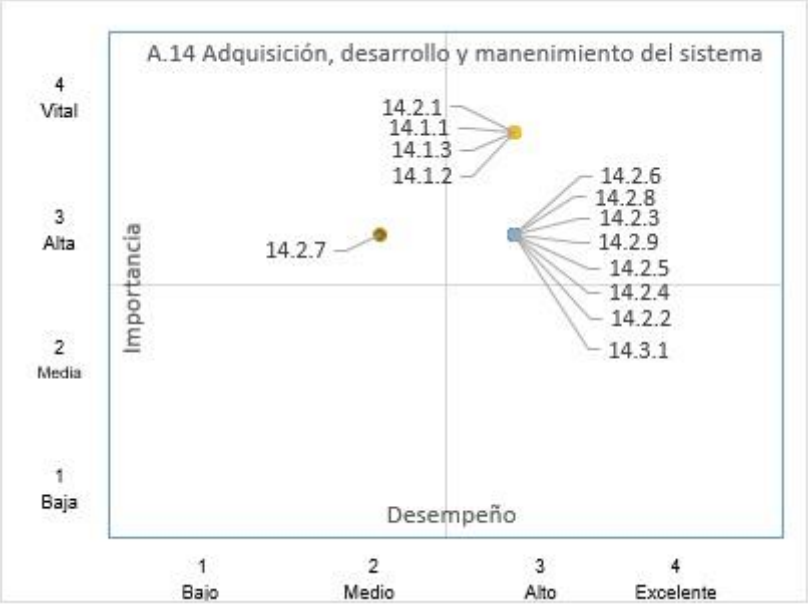


Gráfico 44 Posicionamiento controles objetivo A14
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Un control del objetivo A14 tiene desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

- Doce controles tienen desempeño alto o excelente e importancia alta o vital.
    - Acción: Mantener desempeño. Documentar el proceso.

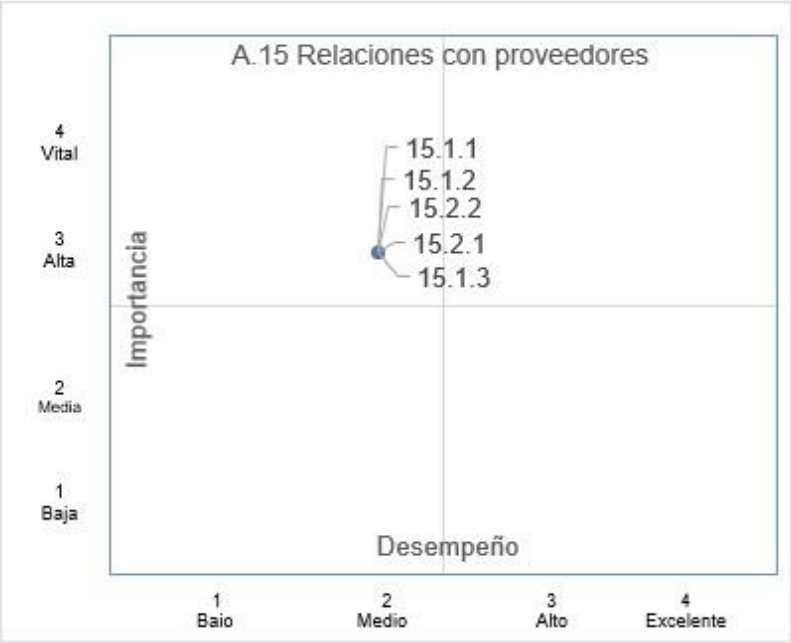


Gráfico 45 Posicionamiento controles objetivo A15
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Cinco controles del objetivo A15 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

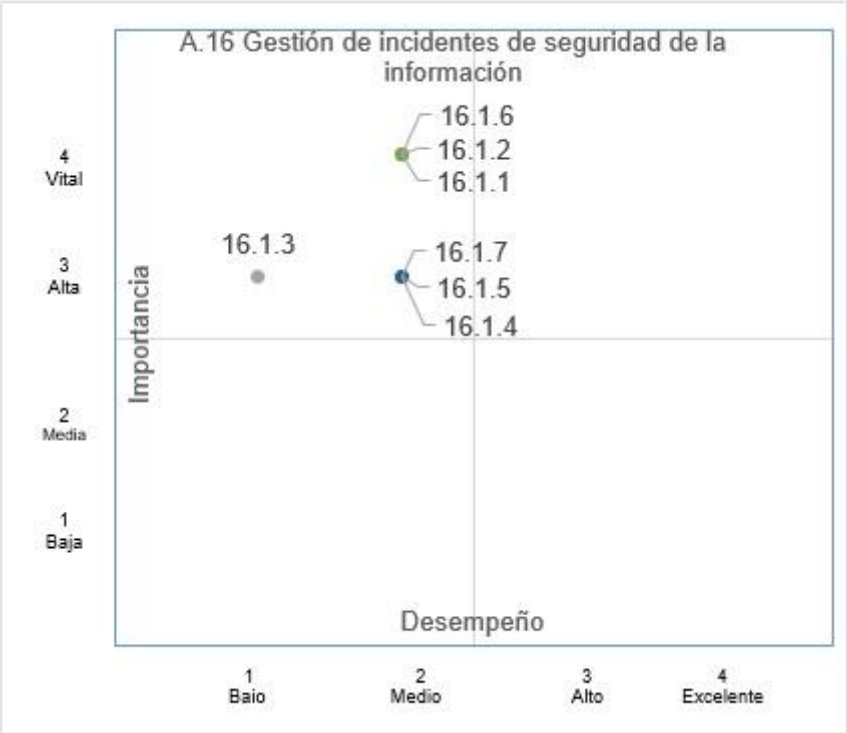


Gráfico 46 Posicionamiento controles objetivo A16
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Siete controles del objetivo A16 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

Gráfico 47 Posicionamiento controles objetivo A17
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Cuatro controles del objetivo A17 tienen desempeño alto o excelente e importancia alta o vital.
    - Acción: Mantener desempeño. Documentar el proceso.

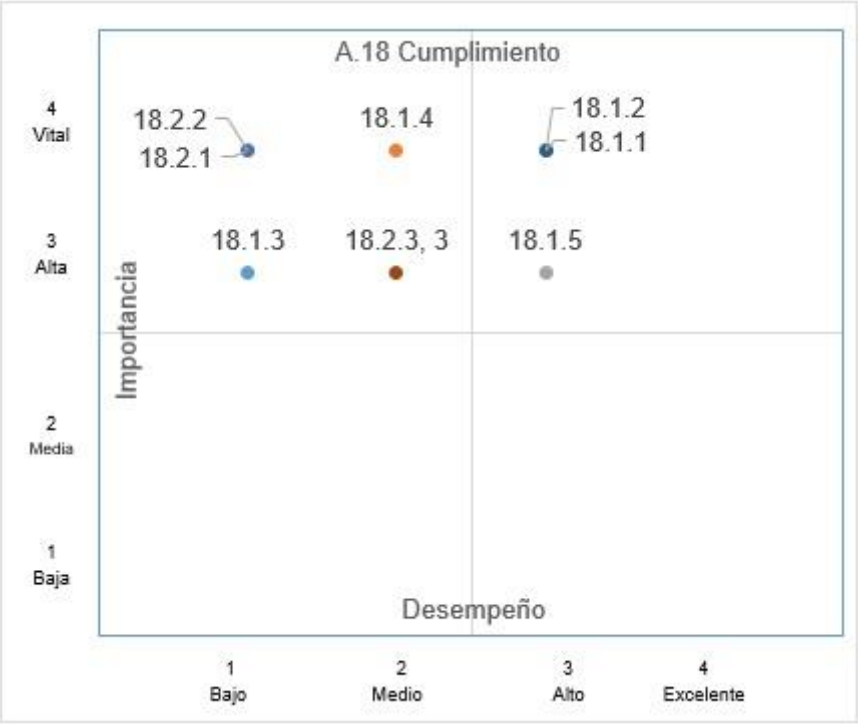


Gráfico 48 Posicionamiento controles objetivo A18
Fuente: Análisis Posicionamiento controles de seguridad
Elaborado por: La investigadora

- Cinco controles del objetivo A18 tienen desempeño bajo o medio e importancia alta o vital.
    - Acción: Priorizar atención. Plan de intervención

- Tres controles tienen desempeño alto o excelente e importancia alta o vital.
    - Acción: Mantener desempeño. Documentar el proceso.

3. Gestión de Seguridad de la Información

La gestión de seguridad de la información propuesta para la Unidad Técnica de Control Académico de la UNACH, se sustentan en la identificación y evaluación de los activos de información, así como el posicionamiento de los controles de seguridad; lo cual permite diferenciar las acciones que requieren atención prioritaria de las que requieren monitoreo.

La propuesta se sustenta en la aplicación de las normas NTE INEN ISO/IEC 27001:2013, 27002:2013 y 27005:2012, configurando el marco normativo, sistemático y metodológico para la gestión de la seguridad de la información.

La gestión de seguridad de la información está agrupada para su trabajo, en secciones conforme cuatro grandes grupos que abarcan el contexto global de requerimientos de la seguridad: Gestión de Activos, Regulaciones, Gestión de Incidentes, Monitoreo y continuidad.

I. Gestión de activos

Objetivo: Establecer el marco metodológico para la identificación, clasificación, evaluación, y tratamiento de los riesgos de seguridad respecto a los activos de información.

Referencia normativa:

- NTE INEN ISO/IEC 27005:2012. Numerales 7 al 12.
- NTE INEN ISO/EC 27002:2013. Objetivo de seguridad 8. Gestión de activos.

Metodología:

1. ***Definición y alcance. -*** Delimitar las áreas, funciones o procesos contemplados en la gestión de activos de información y que contenga:

    a. *Objetivo de la implementación:* La razón que sustenta la implementación de gestión de riesgos respecto a los activos como, por ejemplo: soporte a procesos de gestión de seguridad de la información, continuidad del negocio, plan de atención de incidentes, cumplimiento de procesos relacionados, eficiencia en la gestión de seguridad, etc.

    b. *Misión y giro del negocio:* Que permita identificar los objetivos, políticas y procesos de la unidad y que tienen directa relación con la sensibilidad y criticidad de la información que se maneja.

    c. *Normativa legal que soporta los procesos:* Lo que permite establecer el que contexto legal en el que se desarrollan los procesos para determinar su alcance y limitaciones.

    d. *Restricciones:* Que establecen los límites de operación del proceso y puede ser:

        i. Preexistentes: condiciones, procesos o directrices previamente establecidas sobre las que se debe desarrollar la implementación.

        ii. Técnicas: relacionadas con la infraestructura que posee la unidad para su gestión como software, hardware, redes de comunicación, paquetes de software, archivos, etc.

        iii. Económicas: Conforme el presupuesto priorizado para gestión en seguridad de la información.

        iv. Tiempo: Plazo estimado de ejecución, que no debe ser muy prolongado por la evolución constante de las amenazas.

v. Recursos humanos: cantidad de personal para la gestión de la seguridad, capacitación y entrenamiento, responsabilidades.

2. **<u>Identificación de activos. –</u>** Los activos son de dos tipos: primarios y de soporte.

   a. *Primarios:* son los procesos y la información.

      En los procesos debe considerarse aquellos cuya pérdida afecta al cumplimiento de los objetivos institucionales, o reglamentarios.

      En la información se debe considerar la vital para la ejecución de la misión, la confidencial y estratégica que implique un alto costo de recuperación en caso de pérdida.

      La información también se puede clasificar en confidencial, interna y pública.

   b. *Soporte:* Hardware, software, redes de comunicación, personal.

   Son los activos sujetos a vulnerabilidades que pueden ser explotados por amenazas que buscan afectar los activos primarios.

   Los activos deben ser identificados, asignados a un custodio, clasificados por su nivel de sensibilidad y etiquetados para una adecuada gestión. Los custodios pueden ser una persona o una unidad.

3. **<u>Identificación de amenazas. –</u>** Se debe establecer un listado de todas las posibles amenazas que pueden afectar a los activos de información tipificándolas por ejemplo de procedencia del Recurso Humano, Software y Hardware. Así mimo se puede considerar su origen como deliberadas (ocasionadas con la intención de sustraer, alterar o impedir el acceso a la información), accidentales (por negligencia o falta de capacitación de los usuarios) o naturales (riesgos naturales fuera del control de la institución).

De forma adicional se puede empatar las amenazas identificadas con las posibles vulnerabilidades que crearían el escenario oportuno para que se produzca un incidente de seguridad.

En esta etapa se debe considerar las vulnerabilidades técnicas que puedan poseer los sistemas, para cuya detección se puede apoyar de herramientas de detección de vulnerabilidades y pruebas de penetración.

4. **Valoración de activos. –** Mediante una escala que permita realizar una valoración de acuerdo al criterio de selección que establezca la unidad. La escala puede ser de 3 tipos: cualitativa, cuantitativa o una composición de las dos anteriores.

   La escala de medición puede poseer los niveles que la organización decida, considerando que a mayor número de niveles se vuelve más complejo categorizar los activos.

   La escala de valoración puede ser en función de diversos factores como costo o tiempo de reposición, imagen institucional, interrupción de servicios, confidencialidad, integridad y disponibilidad, etc.; siempre considerando el impacto que sufriría el giro del negocio con un incidente de seguridad.

   Se debe considerar que cada activo de información puede tener diferentes valores, en función de las diferentes amenazas que se identifiquen, lo pueda afectar.

5. **Identificación de controles existentes. –** Que ayude a no duplicar esfuerzos y valorar el nivel de efectividad de los ya existentes. Los controles deben ser valorados por su nivel de madurez respecto a la gestión de seguridad esperada.
6. **Tratamiento del riesgo. –** Que permita decidir si el riesgo será retenido, reducido, evitado o transferido, mediante un plan de tratamiento.

a. *Reducir el riesgo:* selección e implementación de controles que permitan prevenir la ocurrencia del riesgo, considerando sus restricciones respecto a: costo, tiempo, capacitación, infraestructura, etc.

b. *Evitar el riesgo:* Implica dejar de ejecutar una actividad o cambiar su proceso de ejecución en consideración al costo de recuperación del activo y su beneficio.

c. *Transferir el riesgo:* Soporte externo para la gestión de seguridad como por ejemplo contratación de seguros, almacenamiento en la nube, monitoreo, etc. Aquí se debe considerar que el impacto del riesgo no es transferible.

d. *Retener el riesgo:* Es el estado en el que la unidad decide no implementar una acción posterior, principalmente porque el nivel del riesgo es bajo. A este estado deben llegar todos los riesgos.

   En cualquier escenario el plan de gestión de riesgos debe ser conocido y aceptado por el nivel directivo para su respectivo monitoreo.

7. **<u>Monitoreo</u>. –** Al no ser los riesgos estáticos, se debe contar con un plan de monitoreo que determine la periodicidad en la que activos, amenazas, vulnerabilidades y evaluación de riesgos deban ser revisados para determinar cambios en el funcionamiento actual.

El monitoreo permite controlar el ciclo de vida de los riesgos respecto a los activos de información, y garantiza la continuidad del proceso de gestión.

En regulaciones se aborda la definición de políticas respecto al uso de activos.

Plan de acción:

Tabla 17 Plan de acción reducción de riesgos activos de información

Tipo de activo	Activo de Información	Amenaza	Evaluación del riesgo	Tratamiento
primario	Información personal Información académica Información estratégica Personal	Ingeniería social	6	Capacitación a usuarios en seguridad de la información. Al menos 2 eventos al año al inicio de cada ciclo lectivo.
primario	Información personal Información académica Información estratégica	Intrusos	6	Revisión de privilegios de acceso. Monitoreo registros de la base de datos Monitoreo a la red de comunicaciones Pruebas de vulnerabilidad.
primario	Información personal Información académica Información estratégica Personal	Uso no autorizado	6	Acuerdo de confidencialidad para todos los usuarios de los sistemas de información, que incluya responsabilidades, uso aceptable de la información y sanciones.
soporte	Servidor de Base de Datos	Capacidad	6	Control de tiempos de respuesta. Revisión de configuración de consultas. Evaluar la actividad de los usuarios. Depurar componentes, procedimientos almacenados, auditorías. Escalabilidad.
soporte	Servidor de Base de Datos	Comunicaciones	6	Revisar configuraciones de conexión. Privilegios por red. Puertos habilitados. Protocolos de servicio. Vlans
soporte	Servidor de Aplicaciones	Intrusos	6	Revisión de privilegios de acceso. Monitoreo a la red de comunicaciones Pruebas de vulnerabilidad. Revisión registros del sistema.
soporte	Servidor de Aplicaciones Sistemas Red de comunicaciones	Comunicaciones	6	Revisar configuraciones de conexión. Privilegios por red. Puertos habilitados. Protocolos de servicio. Vlans
soporte	Unidades de almacenamiento externo	malware	6	Política de uso. Concienciación a los usuarios.
soporte	Unidades de almacenamiento externo	Robo/hurto	6	Política de uso respecto a la responsabilidad de los custodios de los activos
soporte	Unidades de almacenamiento externo	Daño	6	Política de uso. Respaldo de información

Tipo de activo	Activo de Información	Amenaza	Evaluación del riesgo	Tratamiento
soporte	Sistemas Red de comunicaciones	Falta de personal	4	Identificación de la necesidad, propuesta de potenciación de la unidad.
soporte	Red de comunicaciones	Capacidad	5	Gestión del ancho de banda. Redundancia
soporte	Red de comunicaciones	Falsificación derechos	6	Monitoreo de la actividad de los usuarios. Monitoreo de la red. Pruebas de vulnerabilidad.
soporte	Personal	Negligencia	6	Capacitación a los usuarios. Políticas de uso respecto a la responsabilidad en el manejo de la información Acuerdo de confidencialidad.

Fuente: Matriz de gestión de riesgos activos de información
Elaborado por: La Investigadora

II. Regulaciones

Objetivo: Establecer el marco normativo que debe ser implementado para la adecuada gestión de la seguridad de la información.

Referencia normativa:

- NTE INEN ISO /IEC 27002:2013. Objetivos de seguridad: A5. Política de seguridad de la información; A6. Organización de seguridad de la información; A7. Seguridad en Recursos Humanos; A8. Gestión de activos; A9. Control de acceso; A10. Criptografía; A11. Seguridad física y del entorno; A12. Seguridad en las operaciones; A13. Seguridad en las comunicaciones; A14. Adquisición, desarrollo y mantenimiento del sistema; A15. Relación con proveedores; A18. Cumplimiento.

Metodología

1. **Cumplimiento de la normativa legal. –** Toda acción orientada a la gestión de la seguridad de la información debe partir desde las leyes,

reglamentos y disposiciones externas e internas que son de cumplimiento obligatorio para la institución.

En este contexto, se deberá considerar necesariamente las directrices de protección de propiedad intelectual y de confidencialidad de la información personal, así:

a. *Propiedad intelectual:* Que regule el uso permitido respecto a los activos de información, considerando, por ejemplo:

- Identificar los activos de información que requieran protección de propiedad intelectual, su uso autorizado y referenciación (primarios).
- Software que puede ser instalado y utilizado en los equipos institucionales. Control de licencias utilizadas y disponibles.
- Protección de los registros de información por ejemplo de bases de datos, transacciones, auditorías; su ciclo de vida, medios de protección y responsables.

b. *Datos personales:* En apego a la legislación vigente nacional y acuerdos internacionales, se debe establecer las directrices de privacidad y protección de información personal, en apego a:

- Roles y responsabilidades respecto al procesamiento de información personal.
- Corresponsabilidad de todos quienes manejan información de carácter personal, en la privacidad de su uso, a través de los acuerdos de confidencialidad.
- Se puede sustentar la gestión de la información personal en la norma ISO/IEC 29100.

2. **Política de gestión de la seguridad de la información. –** Implementar la política de seguridad de la información, con base a las normativas y regulaciones que afectan el giro del negocio, en la cual se debe

considerar: alcance, responsabilidades, procedimientos, actualización, evaluación y mejora.

La política de seguridad debe ser aprobada, socializada y estar disponible para todos los interesados.

La política de seguridad puede contener los siguientes apartados:

a. Organización Interna

Que establezca los responsables y procedimientos para el despliegue de la seguridad de la información, estableciendo:

- Procedimiento para la asignación de roles y responsabilidades, tanto físicos como lógicos, respecto a los activos de información.
- Documentar el proceso de gestión de privilegios de acceso. Incluye asignación, modificación, revisión y revocación. La institución debe garantizar que todo cambio interno sea previamente notificado al área pertinente para la modificación de privilegios de acceso.
- Documentar el proceso de gestión de privilegios para administradores de información, su nivel de acceso y responsabilidades.
- Documentar las directrices de seguridad respecto al acceso y manipulación de equipos en el centro de datos institucional, usuarios con privilegio, normas de seguridad, registro de equipos que ingresan y salen, equipos y artefactos permitidos (que no puedan producir interferencia o daño).
- Documentar las directrices respecto al ingreso de usuarios al Centro de Tecnología, considerando procedimientos de registro, verificación de identidad, actividad a desarrollar y salida.
- Documentar el proceso de estándares de seguridad implementados para el Centro de Datos.
- Documentar el flujo del proceso respecto a la notificación de incidentes de seguridad y sus responsables.
- Documentar el proceso de gestión de vulnerabilidades respecto a las alertas que se recibe a través del CSIRT de CEDIA y sus responsables.

- Determinar la responsabilidad de supervisión de vulnerabilidades técnicas en cumplimiento de las actualizaciones de seguridad disponibles.
- Determinar las responsabilidades y procedimientos de uso de dispositivos móviles, así como las garantías de seguridad que deben cumplir, incluyendo: registro, restricciones de instalación de software, protección contra malware, protección de información (credenciales de acceso, criptografía, etc.).
- Determinar responsabilidades y procedimientos para conexión a la administración de los sistemas desde del exterior de la institución, que considere: seguridad en las comunicaciones, equipos permitidos para su uso, procesos que pueden ser ejecutados. Se debe documentar las autorizaciones emitidas para este tipo de casos.
- Documentar el procedimiento de aplicación de controles criptográficos, responsables, vigencia y monitoreo.
- Documentar el proceso de gestión de contraseñas de usuarios, considerando: robustez, cantidad y caracteres permitidos, tipos de mensajes de error.
- Documentar y actualizar los manuales técnicos y de usuario respecto a la gestión de sistemas.
- Preparar, ejecutar y monitorear los resultados del plan anual de mantenimiento de recursos tecnológicos.
- Documentar la gestión de capacidades de los recursos tecnológicos, que contemple: requisitos de seguridad, criticidad, directrices de optimización, monitoreo, depuración de datos, optimización de consultas, etc.
- Determinar los responsables, periodicidad y procedimientos de gestión de copias de seguridad de la información, su clasificación, etiquetado, almacenamiento y disposición final.
- Documentar los procesos de auditoría que se requieran implementar en la gestión de los sistemas de base de datos, su monitoreo y evaluación, siempre en consideración a no afectar la disponibilidad de los sistemas.

b. Recursos Humanos

Que establezca las responsabilidades del personal respecto a la gestión de la información, la idoneidad para el desempeño del cargo y la capacitación requerida para su desempeño óptimo, considerando:

- Determinar los perfiles y experiencia que debe cumplir el personal técnico de programación, administración y soporte a los procesos de gestión de seguridad.
- Establecer los acuerdos de confidencialidad respecto al uso de información institucional, la propiedad del activo, las sanciones por uso negligente o no autorizado inclusive al finalizar la relación contractual.
- Previo inicio de labores el personal debe haber aceptado y firmado el acuerdo de confidencialidad, así como debe recibir por escrito los roles y privilegios de acceso que tiene respecto al manejo de información.
- El recurso humano cumple una doble función dentro de la gestión de seguridad: es activo de soporte de información y puede ser una amenaza para dicha seguridad; de allí que, la institución debe considerar dentro de este proceso el plan de capacitación y concienciación a usuarios respecto a la seguridad.

  Los planes de capacitación deben abarcan los siguientes puntos importantes: uso del sistema, seguridad en el manejo de información, responsabilidad sobre el uso de la información, obligación de notificar posibles vulnerabilidades del sistema, concienciación respecto a los activos de información y políticas de seguridad que maneja la institución.

  El plan de capacitación debe considerar periodicidad, campañas de concienciación, y temáticas relevantes de gestión, de forma opcional se puede considerar una evaluación que garantice la transferencia de conocimientos.

  El plan de capacitación también debe considerar la actualización en conocimientos al personal técnico que da soporte a los procesos de seguridad.

c. Activos de información

El complemento a la gestión de activos de información deben ser las regulaciones respecto al uso de los activos y las responsabilidades de los custodios y usuarios, así:

- Establecer y socializar procedimientos respecto a la custodia, traslado y manipulación de activos, que garanticen no únicamente el activo de soporte (equipos portátiles, tabletas, etc.), sino la responsabilidad sobre el activo primario que es manipulado en dichos equipos y que podría ser comprometida en caso de uso negligente, robo o hurto.

  Este procedimiento debe contemplar la propiedad intelectual de los activos primarios, los derechos de uso aceptable de la información y sus activos de soporte asociado.
- Para la gestión de activos es necesario normalizar la clasificación y etiquetado de activos, respecto a su nivel de sensibilidad o usabilidad.
- Establecer las directrices respecto a la responsabilidad, uso, modificación, salida de la institución, borrado y eliminado de medios extraíbles que se contengan activos primarios de información.

d. Comunicaciones

Que establezca las políticas y procedimientos de seguridad respecto a la gestión de comunicaciones.

- Documentar la responsabilidad de los técnicos de gestión de redes, su atribuciones y procesos asociados.
- Determinar las directrices de acceso y privilegios por usuario respecto a los servicios de comunicación, que incluya la responsabilidad y uso de la infraestructura de comunicaciones.
- Documentar el procedimiento de gestión de redes y sus dominios.
- Documentar los procedimientos y protocolos de seguridad que garantizan la transferencia información a través de las redes de comunicación.
- Determinar la gestión de procedimientos criptográficos que aseguren las comunicaciones y protejan la información de afectaciones en la confidencialidad, integridad, disponibilidad y confiabilidad.

- Determinar las directrices respecto a descarga y utilización de software en equipos institucionales.
- Determinar las directrices respecto a puertos y protocolos de comunicación habilitados conforme los privilegios de utilización de red por parte de los usuarios.
- Documentar las directrices respecto al uso de los servicios de mensajería electrónica institucional y la información transferida por estos medios.
- Documentar las directrices respecto a las configuraciones de seguridad de los equipos tecnológicos de soporte que operan a través de redes interconectada como por ejemplo impresoras, fax, telefonía IP, etc.

e. Gestión de proyectos de desarrollo y mantenimiento de sistemas

Que regule todo el ciclo de vida del desarrollo, mantenimiento o actualización de sistemas.

- Documentar los procedimientos de gestión de proyectos de desarrollo de software, incluyendo la gestión de la seguridad de la información, a lo largo de todos los procedimientos asociados.

  El desarrollo externalizado debe cumplir las mismas características de seguridad.
- Documentar los requisitos de seguridad que deben cumplir los sistemas en producción ya sean de uso interno o acceso web.
- Documentar los procedimientos de gestión de certificados digitales, responsables y ciclo de vida.
- Documentar los procedimientos de pruebas y control de cambios que garanticen la usabilidad de los sistemas, previa su operación en producción, evaluando riesgos e impactos, control de versiones, actualización de manuales.

  Se debe garantizar que las pruebas se ejecutan en ambientes separados a los de desarrollo y producción y la seguridad respecto a los datos de prueba utilizados, su acceso, manipulación y eliminado.

- Establecer directrices respecto a la utilización de principios de ingeniería de sistemas seguros que contemplen técnicas de autenticación, conexiones seguras, validación de datos, depuración de código, etc.
- Determinar las directrices respecto a los procedimientos, validación y control de cambios para pruebas de seguridad y pruebas de aceptación.

f. Proveedores

Determinar los procedimientos seguros de manejo de información con proveedores.

- Identificar y documentar los tipos de proveedores que requiere el giro del negocio, como: servicios de comunicación, equipamiento, consultoría, paquetes de software, de desarrollo, etc.

  El determinar el tipo de proveedores permite establecer las regulaciones de seguridad en la relación contractual con cada uno de ellos.

  Dentro de la relación de con proveedores se debe considerar los acuerdos de confidencialidad y uso de información, cuando la relación contractual así lo requiera.
- Se debe documentar los requisitos de seguridad que deben cumplir los productos o servicios que son contratados a terceros.
- La documentación de soporte para los procesos de contratación debe contemplar los requisitos de seguridad esperados sobre los productos o servicios, como actualización tecnológica, cumplimiento de estándares, garantía, soporte, mantenimiento, etc.

g. Incidentes de seguridad

- Determinar las regulaciones respecto a la gestión de incidentes de seguridad que contemple: planificación, evaluación y toma de decisiones.

Las regulaciones deben contemplar la necesidad de documentar los incidentes de seguridad para su monitoreo, aprendizaje y retroalimentación.

Se debe establecer formatos homologados que permitan documentar lo incidentes de seguridad.

Además, se debe establecer el canal de comunicación y periodicidad para notificar los incidentes de seguridad al nivel jerárquico superior y estratégico conforme la criticidad de los eventos suscitados.

- Determinar los procesos disciplinarios asociados a un incidente de seguridad por uso negligente o no autorizado respecto a los activos de información.

III. Gestión de Incidentes de seguridad

Objetivo: Establecer el marco metodológico para la gestión de incidentes de seguridad.

Referencia normativa:

- NTE INEN ISO/IEC 27002:2013. Objetivo de seguridad A16. Gestión de incidentes de seguridad de la información

Metodología:

1. **Responsables. -** Se debe establecer los responsables respecto a gestión de incidentes de seguridad, la línea de comunicación y acción.

2. **Plan de acción. –** que contemple los procedimientos para monitorear, detectar, analizar y documentar los incidentes de seguridad.

   El proceso de monitoreo y detección de eventos de seguridad permite valorar si la sensibilidad de un evento de seguridad requiere ser

catalogado como incidente para su respectivo tratamiento, notificación y documentación.

El plan de acción debe contener los procedimientos de respuesta a incidentes de seguridad y su tratamiento.

El plan de acción debe ser aprobado por el directivo de la unidad.

3. **Notificación. –** Cuando el tratamiento requerido excede las posibilidades de la unidad, se debe escalar la propuesta de solución al nivel estratégico para su aprobación respecto a los requisitos para mitigar el incidente.

   Los eventos de seguridad deben ser clasificados por su criticidad para evaluar los que requieran ser notificados, como, por ejemplo: inseguridad en las comunicaciones, afectación a la confidencialidad, integridad o disponibilidad, negligencia, incumplimiento de directrices, falla de software o hardware, accesos no autorizados, etc.

   La notificación de eventos de seguridad debe incluir al personal, quienes deben tener la responsabilidad de anotar y notificar cualquier debilidad o falla de seguridad que se identifique respecto a los sistemas.

4. **Respuesta. –** Que recupere la fiabilidad respecto a la seguridad de la información y que considere: recolección de evidencias, análisis forense, escalado de incidentes, tratamiento de la debilidad y cierre del incidente. Todo esto de forma documentada para su posterior análisis y reducción de posibilidades de futuras ocurrencias.

IV. Monitoreo y continuidad

Objetivo: Garantizar que la gestión en seguridad se cumpla conforme ha sido establecida, se actualiza y adapta a los nuevos riesgos y necesidades y se mantiene en el tiempo como un proceso transversal a lo largo de la gestión de procesos institucionales.

Referencia normativa:

- NTE INEN ISO/IEC 27002:2013. Objetivo A17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio.
- NTE INEN ISO/ IEC 27005:2013. Anexo D.

Metodología:

1. **Monitoreo:**

   Para un adecuado monitoreo es necesario se proyecte la ejecución de planes de: supervisión a las actividades de los administradores, mantenimiento de infraestructura hardware, sistemas, redes de comunicación, gestión de riesgos, capacitación y actualización de controles y políticas de seguridad.

- Las acciones del personal administrador deben ser supervisadas por el nivel directivo, no únicamente respecto a los privilegios de acceso que tienen sino a las acciones ejecutadas con dichos privilegios. Un monitoreo periódico de que los procedimientos se cumplan conforme han sido dispuestos y aprobados es necesario para mantener un adecuado control respecto a la seguridad de la información.

- Los planes de mantenimiento deben ser documentados, formalmente validados y aprobados por un nivel jerárquico superior, el cual debe

contener los responsables, objetivos, alcance, tiempo de ejecución y resultados esperados.

Un plan de mantenimiento debe considerar la actualización de software, parches de seguridad, depuración de código, revisión de seguridad física y lógica, optimización de recursos, privilegios de acceso, entre otros; siempre garantizando la disponibilidad de los servicios.

- La gestión de riesgos ya analizada en la sección I, forma parte del monitoreo considerando que los activos de información deben contar con un plan de actualización, evaluación y tratamiento, que garantice su fiabilidad.

- Los planes de capacitación también abordados en la sección II, permiten fortalecer la seguridad respecto al recurso humano, disminuyendo vulnerabilidades que puedan afectar a los activos de información.

  Sobre los resultados de la aplicación de estos planes se debe realizar una evaluación orientada a determinar el nivel de eficacia alcanzado, que permita retroalimentar y mejorar el proceso de forma permanente.

- La actualización de controles de seguridad si bien es cierto pueden formar parte de los planes de mantenimiento, se abordan de manera separada considerando la importancia que tiene la gestión de los mismos.

  Los controles de seguridad deben contar con un plan que garantice su identificación, procedimiento de aplicación, actualización y mejora.

  Para sustentar los resultados del monitoreo a los controles de seguridad implementados, es importante complementar este proceso con la ejecución de pruebas de vulnerabilidad y/o penetración, que confirman el grado de seguridad considerado por la institución.

- La actualización de políticas de seguridad depende precisamente de un proceso de identificación, aplicación y evaluación de resultados obtenidos

que permita tomar decisiones sobre aquellas que sean susceptibles a ser mejoras, estén obsoletas o deban mantener su funcionamiento.

Las políticas de seguridad deben ser revisadas, actualizadas y aprobadas; sin embargo, no constituyen un documento inanimado que deba permanecer guardado; por ello es fundamental que su socialización permanente sea parte de los planes de capacitación y comunicación institucional, abordándose su jerarquía no únicamente como un frío conjunto de obligaciones a cumplir, sino elevando su importancia a un nivel de corresponsabilidad y empoderamiento con la seguridad de los activos de información institucional.

2. Continuidad:

La continuidad es el procedimiento que garantiza que la gestión de seguridad de la información no constituya un conjunto de buenas intenciones con un inicio impetuoso, que lentamente va agonizando y termina como letra muerta sin utilización. Por ello la misma se orienta a:

El monitoreo y evaluación de resultados obtenidos debe ser utilizado para analizar la gestión de la seguridad de la información en un período determinado de tiempo.

El resultado de este análisis debe permitir tomar las decisiones adecuadas respecto a cómo se manejará la continuidad de la seguridad, respecto a:

- Actualización de controles de seguridad por vulnerabilidades o nuevas amenazas detectadas.
- Mejora en la definición de políticas, procedimientos y directrices de seguridad.
- Actualización de contenidos para el manejo del plan de capacitación y concienciación de usuarios.
- Fortalecimiento del plan de mantenimiento de infraestructura tecnológica.

- Mantener los procedimientos que han dado resultados positivos durante la gestión de seguridad.

El nivel directivo es responsable del monitoreo y continuidad de la seguridad.

6.8 Administración

La gestión de riesgos respecto a los activos de información y el manejo de buenas prácticas en seguridad de la información debe convertirse en un proceso transversal dentro de la gestión de la organización; para ello se requiere:

- Nombrar un equipo multidisciplinario encargado de la elaboración y presentación de las políticas y procedimientos respecto a la seguridad de la información, contar con su aprobación para iniciar la socialización.
- Definir los roles y responsables para la gestión de activos de información, su monitoreo y evaluación.
- Definir los responsables para la elaboración ejecución y evaluación de los planes de seguimiento a las actividades de los administradores, mantenimiento, capacitación, y actualización de controles de seguridad.
- Definir los roles de los responsables del monitoreo y continuidad de la seguridad de la información.
- Integrar la gestión de la seguridad a todas las áreas que corresponden a tecnología para no establecer esfuerzos aislados, sino más bien instaurar una estructura sólida respecto a la seguridad de la información.
- El compromiso del nivel jerárquico superior es fundamental para posicionar la gestión de la seguridad de la información como parte de la gestión de procesos y no únicamente como la mitigación de incidentes de seguridad, que en determinado momento termina resultado más costoso que una gestión en prevención.

Para el despliegue de todo el proceso se han considerado los siguientes plazos, de acuerdo a la complejidad de cada etapa y los procesos de gestión interna que deben ser atravesados, así:

Tabla 18 Cronograma despliegue seguridad de la información

No	Proceso	Tiempo estimado	Observaciones
1	Gestión de riesgos respecto a los activos de información	30 días	La identificación y evaluación de activos de información ya ha sido ejecutada. Se requiere formalizar y sistematizar el proceso.
2	Elaboración y aprobación de políticas y directrices de seguridad de la información	90 días	Con base a los lineamientos establecidos en la gestión de seguridad se debe establecer las políticas que abarquen todo el proceso de seguridad de la información. Conforme sugerencia previa se debe integrar todo la gestión de tecnología en este proceso.
3	Plan de socialización y despliegue	60 días	Planes comunicaciones y de capacitación que lleguen a la mayor cantidad posible de usuarios respecto a las políticas de seguridad que implementa la institución.
4	Implementación de controles de seguridad	60 días	Considerando el tratamiento definido para el riesgo asociado, y en consideración a los costos de implementación que sean aprobados.
5	Monitoreo y evaluación	Permanente	Permanente desde el proceso de implementación pero con énfasis en el momento planificado para determinar los resultados de gestión
6	Mejora y continuidad	Permanente	Que permita determinar los puntos clave de mejora ya sea por necesidad de actualización, controles ineficientes o aplicación de nuevos procedimientos que garantice la continuidad de la seguridad en la información.
Total		**240 días**	Para el despliegue. El monitoreo y la mejora continua no forman parte del despliegue

Elaborado por: La Investigadora

6.9 Previsión de la evaluación

Con la implementación de la gestión de la seguridad y aplicando las recomendaciones por control de seguridad, se prevé el escenario favorable de madurez para cada objetivo de control, así:

Tabla 19 Recomendaciones objetivo A5

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	5.1.1 Política de seguridad de la información para los SGBD	Implementar la política de seguridad de la información, con base a las normativas y regulaciones que afectan el giro del negocio, en la cual se debe considerar: alcance, responsabilidades, procedimientos, actualización, evaluación y mejora. La política de seguridad debe ser aprobada, socializada y estar disponible para todos los interesados. La política de seguridad puede contener los siguientes apartados: a. Organización Interna b. Recursos Humanos c. Activos de información d. Comunicaciones e. Proyectos de desarrollo f. Proveedores g. Incidentes de seguridad
	5.1.2 Revisiones a la política de seguridad	Ejecutar los procesos de monitoreo y continuidad que establece la gestión en seguridad.

Elaborado por: La Investigadora

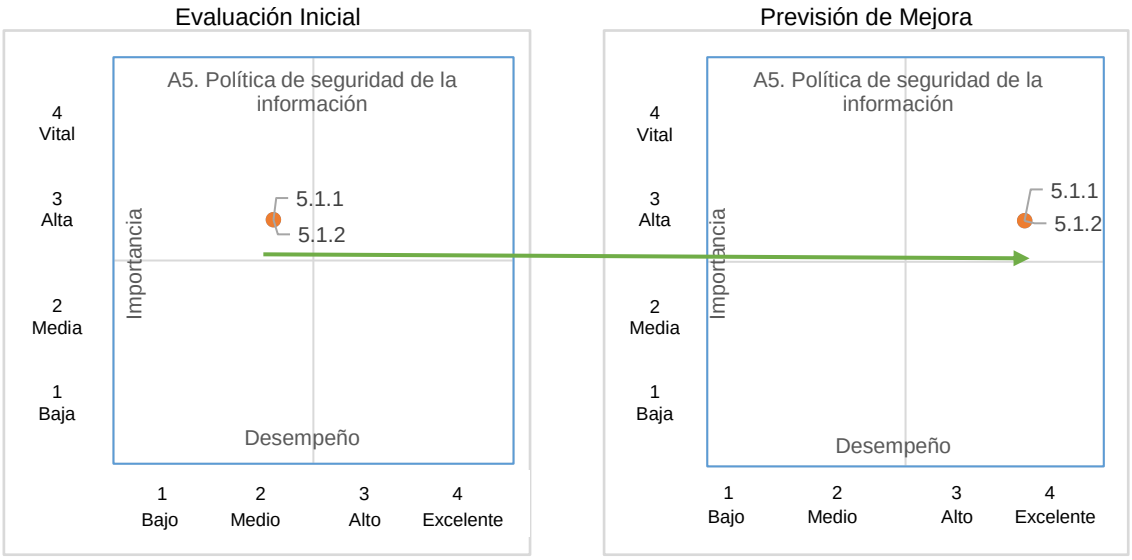


Gráfico 49 Comparación previsión de mejora Objetivo A5
Elaborado por: La Investigadora

La gestión de la seguridad de la información prevé mejorar el desempeño de medio a excelente para los controles con importancia alta o vital.

Tabla 20 Recomendaciones Objetivo A6

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	6.1.1 Roles y responsabilidades de seguridad de la información	Mantener un procesos sistemático respecto a la gestión de activos de información, su evaluación y tratamiento. Documentar los procedimientos de gestión de roles y privilegios de acceso.
	6.1.2 Separación de funciones	Documentar los procedimientos de gestión de roles y privilegios de acceso. Cumplir dentro del proceso de monitoreo y continuidad con el plan de supervisión de los administradores. Documentar la gestión de auditorías de transacciones y su ciclo de vida.
	6.1.3 Contacto con las autoridades	Documentar el flujo de comunicación. Identificar los tipos de proveedores de productos y servicios que tienen relación con el giro del negocio.
	6.1.4 Contacto con grupos de interés especial	Documentar el procedimiento de gestión de alertas que establece el CSIRT de CEDIA, sus responsables y acciones.
	6.1.5 Gestión de Proyecto de seguridad de la información	Implementar la política de seguridad de la información con base a la gestión en seguridad
	6.2.1 Política de dispositivo móvil	Documentar el procedimiento de gestión de privilegios de acceso a la red de comunicación y sistemas. Determinar los procedimientos de seguridad para obtener privilegios de conexión a la red de comunicaciones, desde equipos móviles.
	6.2.2 Teletrabajo	Documentar las responsabilidades, obligaciones y conexiones de seguridad para autorizar acceso externo a la administración de sistemas

Elaborado por: La Investigadora

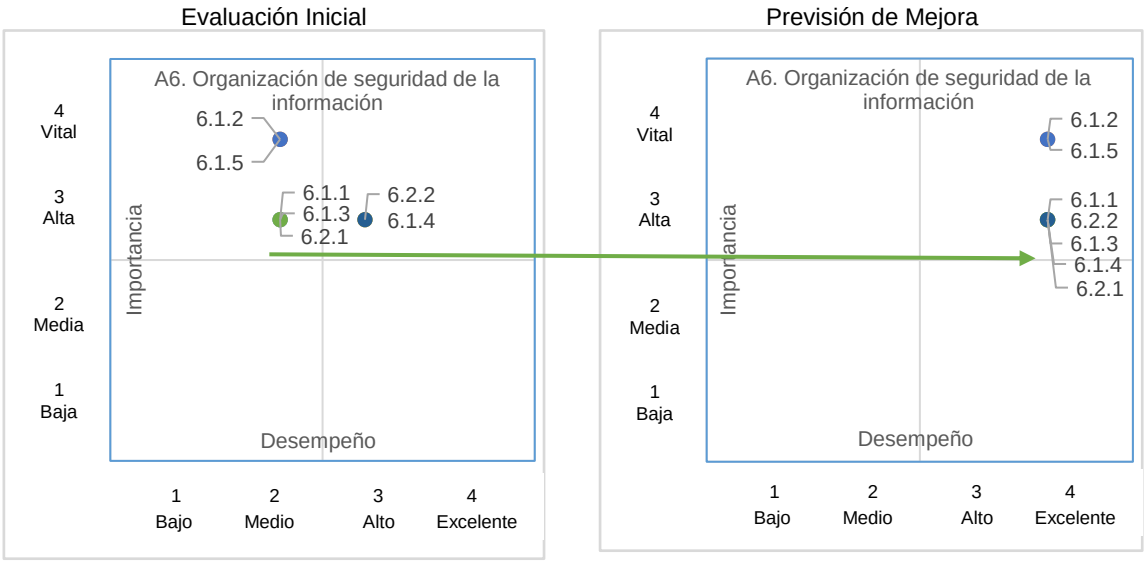


Gráfico 50 Comparación previsión de mejora objetivo A6
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de medio y alto a excelente para los controles con importancia alta o vital.

Tabla 21 Recomendaciones Objetivo A7

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	7.1.1 Investigación de antecedentes 7.1.2 Términos y condiciones laborales	Firma obligatoria de los acuerdos de confidencialidad por parte de todos los usuarios, que incluya propiedad intelectual de los activos, su uso aceptable y responsabilidades incluso al finalizar la relación laboral
	7.2.1 Responsabilidades de la Dirección	Elaborar e implementar el plan de capacitación y concienciación a usuarios respecto a la corresponsabilidad en la seguridad de la información. Considerar de forma alternativa que dicho plan puede ser evaluado para garantizar la transferencia de conocimientos. Parte importante de dicho plan es la actualización en conocimientos del personal técnico que da soporte a los procesos de seguridad.
	7.2.2 Concienciación, educación y formación en seguridad de la información	Forma parte del plan de capacitación las campañas comunicacionales permanentes respecto a la importancia de la seguridad de la información,

	7.2.3 Proceso disciplinario 7.3.1 Responsabilidad por finalización o cambio de empleo	Establecer los acuerdos de confidencialidad respecto al uso de información institucional, la propiedad del activo, las sanciones por uso negligente o no autorizado inclusive al finalizar la relación contractual

Elaborado por: La Investigadora

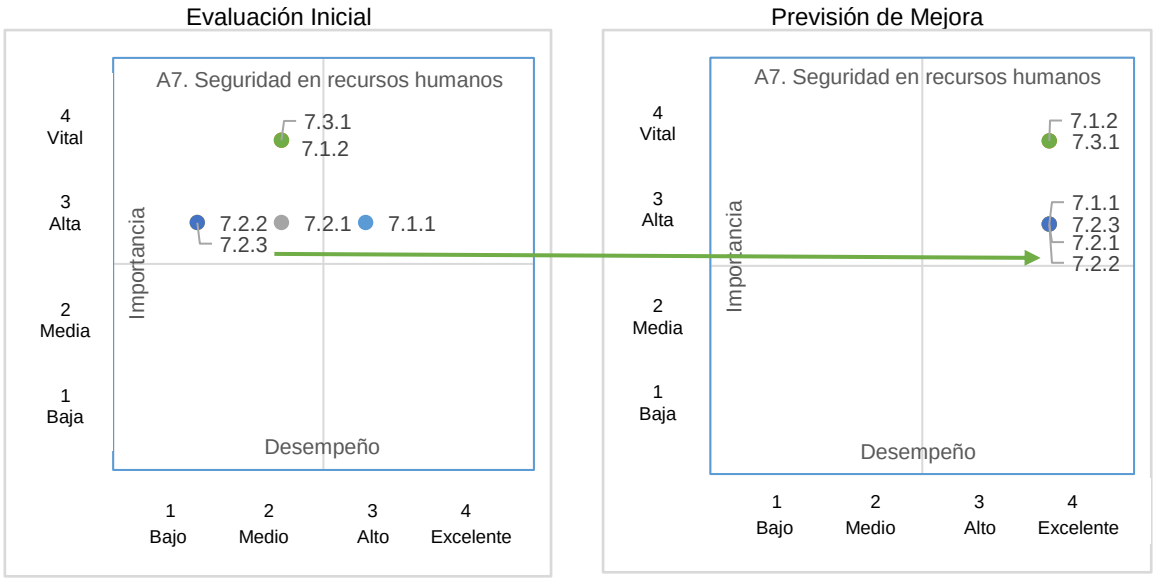


Gráfico 51 Comparación previsión de mejora objetivo A7
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de medio y alto a excelente para los controles con importancia alta o vital.

Tabla 22 Recomendaciones Objetivo A8

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	8.1.1 Inventario de activos	Mantener un procesos sistemático respecto a la gestión de activos de información, su evaluación y tratamiento. Documentar los procedimientos de gestión de roles y privilegios de acceso.
	8.1.2 Propiedad de los activos	Política de uso respecto a la responsabilidad de los custodios de los activos
	8.1.3 Uso aceptable de los activos 8.2.1 Clasificación de la información 8.2.2 Etiquetado de la información	Clasificar la información conforme su nivel de sensibilidad y considerar en el acuerdo de confidencialidad el uso aceptable respecto a las mismas.

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	8.1.4 Devolución de activos 8.2.3 Manejo de activos	Establecer los acuerdos de confidencialidad respecto al uso de información institucional, la propiedad del activo, las sanciones por uso negligente o no autorizado inclusive al finalizar la relación contractual
	8.3.1 Gestión y transferencia de medios extraíbles	Establecer las directrices respecto a la responsabilidad, uso, modificación, salida de la institución, borrado y eliminado de medios extraíbles que se contengan activos primarios de información
	8.3.2 Eliminación de los medios 8.3.3 Transferencia de medios físicos	Documentar el procedimiento de seguridad respecto al uso de medios extraíbles.

Elaborado por: La Investigadora

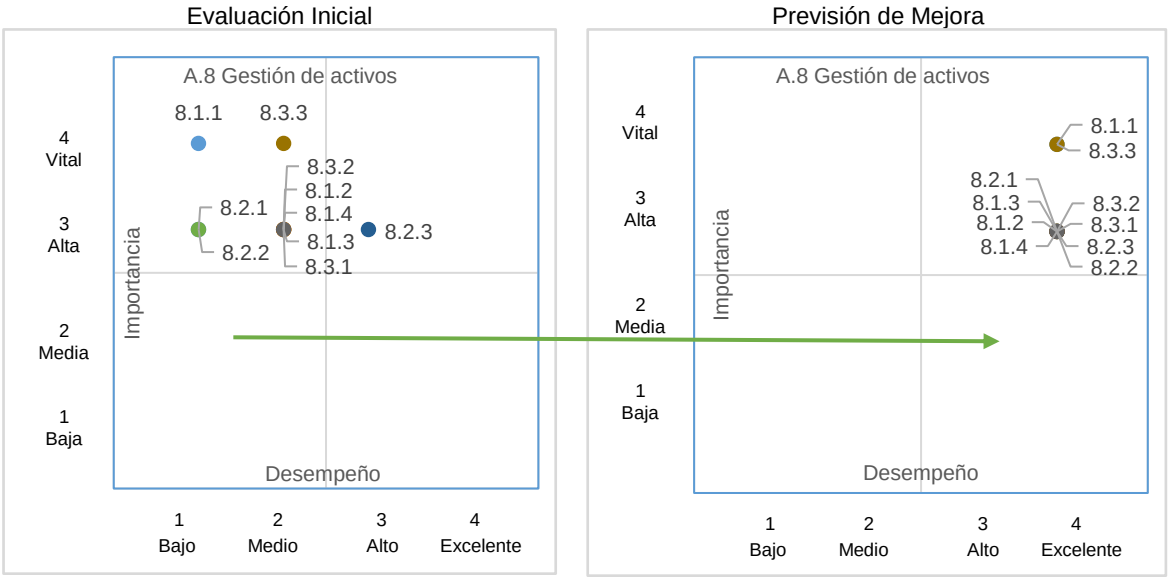


Gráfico 52 Comparación previsión de mejora objetivo A8
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de bajo, medio y alto a excelente para los controles con importancia alta o vital.

Tabla 23 Recomendaciones Objetivo A9

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	9.1.1 Política de control de acceso	Documentar los procedimientos de concesión de privilegios de acceso conforme los requerimientos de cada rol de los usuarios
	9.1.2 Acceso a redes y servicios de red	Documentar los procedimientos de concesión de privilegios de acceso conforme los requerimientos de cada rol de los usuarios Monitorear las acciones de los usuarios.
	9.2.1 Registro y retiro de usuarios 9.2.2 Provisión de accesos a usuarios 9.2.3 Gestión de privilegios de derechos de acceso 9.4.1 Restricción del acceso a la información	Documentar los procedimientos de concesión de privilegios de acceso conforme los requerimientos de cada rol de los usuarios Monitorear las acciones de los usuarios. Establecer los procedimientos de revocación de privilegios.
	9.2.4 Gestión de la información secreta de autenticación de los usuarios	Documentar el procedimiento de autenticación y controles de seguridad que maneja
	9.2.5 Revisión de los derechos de acceso de usuarios 9.2.6 Retiro y ajuste de los derechos de acceso	Considerar dentro de los planes de mantenimiento de sistemas, la revisión de privilegios de acceso conforme roles de usuario.
	9.3.1 Uso de información secreta de autenticación	Considerar dentro de los planes de capacitación la seguridad en el uso de información
	9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Sistema de gestión de contraseñas	Documentar los procedimientos de inicio de sesión y controles de seguridad que soportan una autenticación robusta.
	9.4.4 Uso de programas utilitarios privilegiados	Documentar las directrices consideradas al respecto.
	9.4.5 Control de acceso al código fuente del programa	Documentar el procedimiento respecto al registro en el IEPI

Elaborado por: La Investigadora

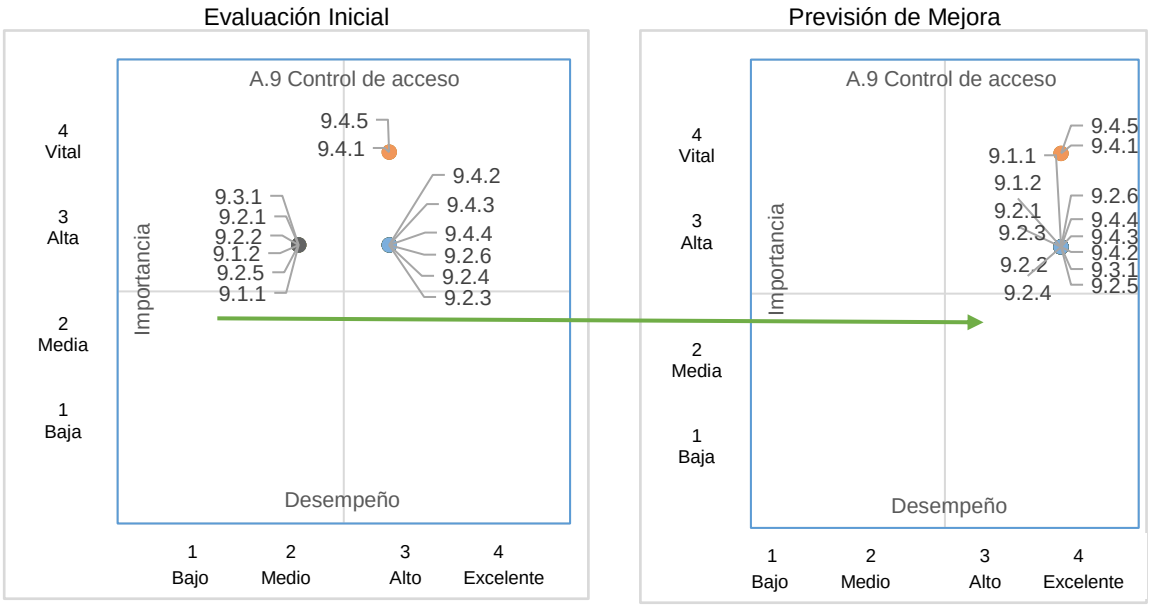


Gráfico 53 Comparación previsión de mejora objetivo A9
Elaborado por: *La Investigadora*

La gestión de seguridad de la información prevé mejorar el desempeño de medio y alto a excelente para los controles con importancia alta o vital.

Tabla 24 Recomendaciones Objetivo A10

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	10.1.1 Política de uso de los controles criptográficos	Documentar el procedimiento de controles criptográficos utilizado para la gestión de contraseñas.
	10.1.2 Gestión de llaves	Documentar el procedimiento de responsables y uso de certificados digitales.

Elaborado por: La Investigadora

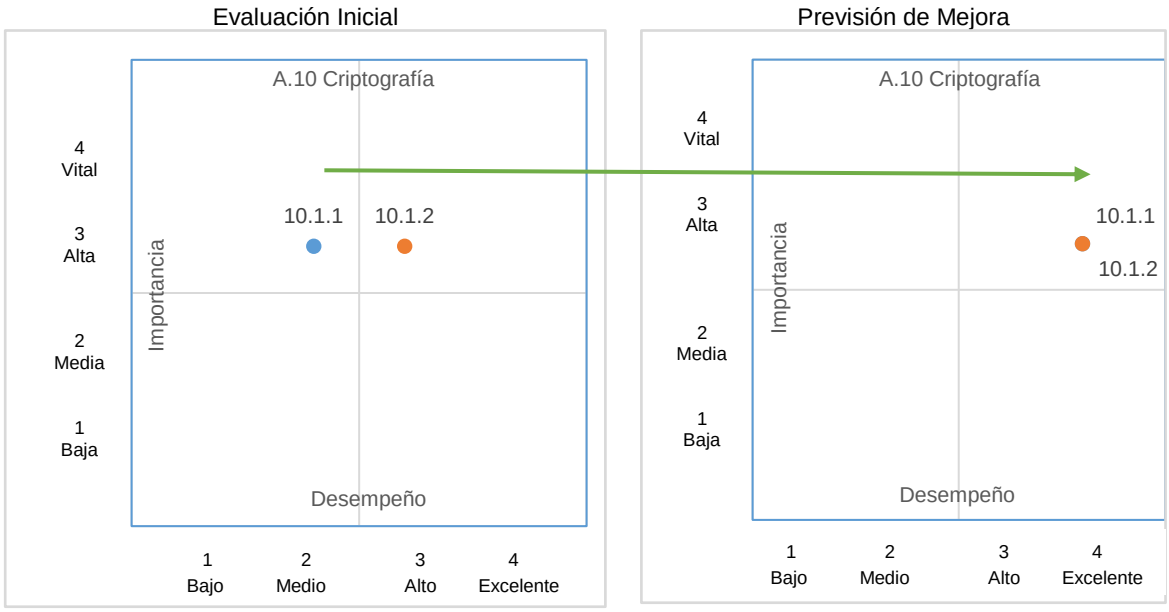


Gráfico 54 Comparación previsión de mejora objetivo A10
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de medio y alto a excelente para los controles con importancia alta o vital.

Tabla 25 Recomendaciones Objetivo A11

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	11.1.2 Controles físicos de entrada	Documentar las directrices de seguridad respecto al acceso y manipulación de equipos en el centro de datos institucional, usuarios con privilegio, normas de seguridad, registro de equipos que ingresan y salen, equipos y artefactos permitidos (que no puedan producir interferencia o daño)
	11.1.3 Seguridad de oficinas, despachos e instalaciones. 11.2.7 Reutilización o eliminación segura de equipos 11.2.8. Equipos de usuario desatendido 11.1.6 Áreas de carga y entrega 11.2.1 Ubicación y protección de equipos 11.2.2 Instalaciones de suministro 11.2.3 Seguridad del cableado	Documentar los controles de seguridad implementados

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	11.2.4 Mantenimiento de los equipos	
	11.1.1 Protección contra las amenazas externas y ambientales	Documentar los procedimientos de gestión de riesgos y cumplimiento de estándares y normativa de seguridad
	11.1.5 Trabajo en áreas seguras	Documentar el procedimiento de gestión de riesgos en seguridad laboral
	11.2.5 Eliminación de activos	Implementar la política respecto a la responsabilidad de uso de activos primarios de información fuera de las instalaciones institucionales. La responsabilidad va más allá de la custodia del equipo.
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	Determinar las responsabilidades y procedimientos de uso de dispositivos móviles, así como las garantías de seguridad que deben cumplir, incluyendo: registro, restricciones de instalación de software, protección contra malware, protección de información (credenciales de acceso, criptografía, etc.).
	11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Considerar estos requerimientos en los procesos de capacitación a usuarios

Elaborado por: La Investigadora

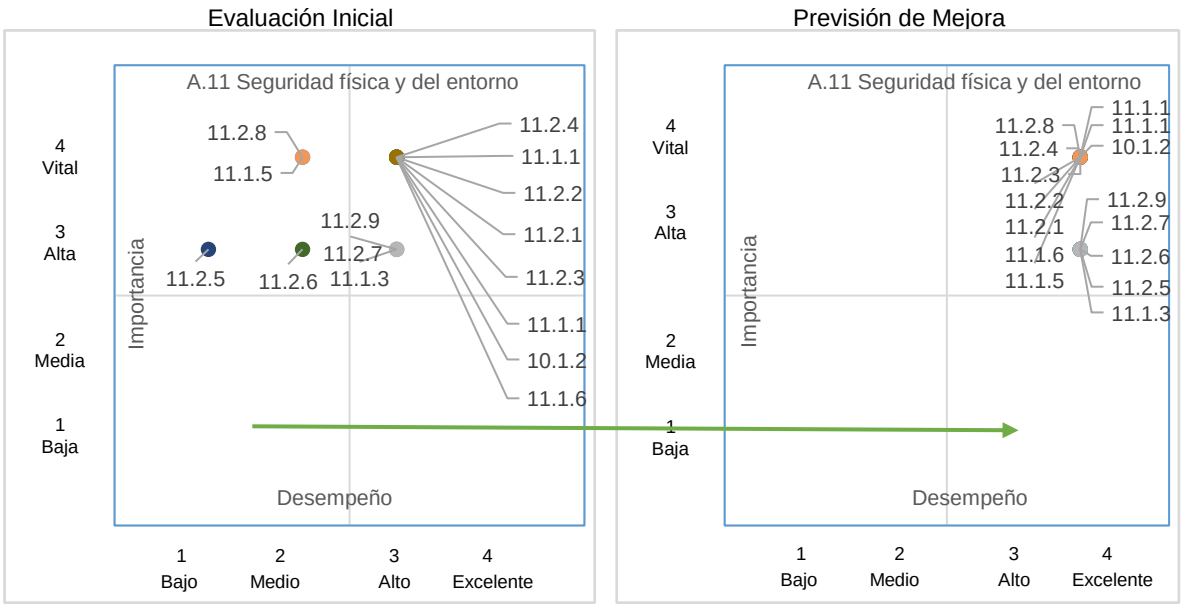


Gráfico 55 Comparación previsión de mejora objetivo A11
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de bajo, medio y alto a excelente para los controles con importancia alta o vital.

Tabla 26 Recomendaciones Objetivo A12

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	12.1.1 Documentación de procedimientos de operación	Documentar y actualizar los manuales técnicos y de usuario respecto a la gestión de sistemas.
	12.1.2 Gestión de cambios	Documentar los procedimientos de pruebas y control de cambios que garanticen la usabilidad de los sistemas, previa su operación en producción, evaluando riesgos e impactos, control de versiones, actualización de manuales.
	12.1.3 Gestión de capacidades	Documentar la gestión de capacidades de los recursos tecnológicos, que contemple: requisitos de seguridad, criticidad, directrices de optimización, monitoreo, depuración de datos, optimización de consultas, etc.
	12.1.4 Separación de ambientes de desarrollo, pruebas y producción	Se debe garantizar que las pruebas se ejecutan en ambientes separados a los de desarrollo y producción y la seguridad respecto a los datos de prueba utilizados, su acceso, manipulación y eliminado.
	12.2.1 Controles contra malware 12.4.4 Sincronización del reloj	Documentar los controles de seguridad implementados
	12.3.1 Copias de seguridad de la información	Determinar los responsables, periodicidad y procedimientos de gestión de copias de seguridad de la información, su clasificación, etiquetado, almacenamiento y disposición final.
	12.4.1 Registro de eventos	Supervisar periódicamente las acciones de los usuarios en los registros de transacciones y pistas de auditoría.
	12.4.2 Protección de la información de registro	Protección de los registros de información por ejemplo de bases de datos, transacciones, auditorías; su ciclo de vida, medios de protección y responsables.
	12.4.3 Registros de administración y operación	Las acciones del personal administrador deben ser supervisadas no únicamente respecto a los privilegios de acceso que tienen sino a las acciones ejecutadas con dichos privilegios. Un monitoreo periódico de que los procedimientos Se cumplan conforme han sido dispuestos y aprobados es necesario para mantener un adecuado control respecto a la seguridad de la información.

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	12.5.1 Instalación del software en los sistemas operativos 12.6.2 Restricciones en la instalación del software	Determinar las directrices respecto a descarga y utilización de software en equipos institucionales.
	12.6.1 Gestión de las vulnerabilidades técnicas	Determinar la responsabilidad de supervisión de vulnerabilidades técnicas en cumplimiento de las actualizaciones de seguridad disponibles.
	12.7.1 Controles de auditoría de sistemas de información	Documentar los procesos de auditoría que se requieran implementar en la gestión de los sistemas de base de datos, su monitoreo y evaluación, siempre en consideración a no afectar la disponibilidad de los sistemas

Elaborado por: *La Investigadora*

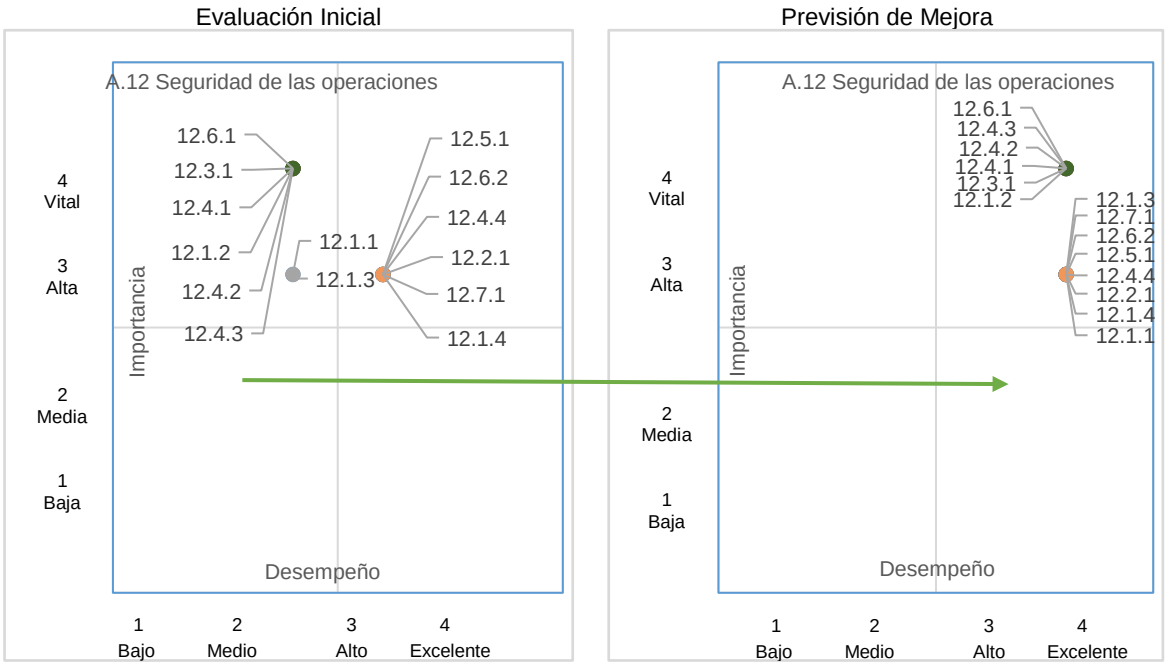


Gráfico 56 Comparación previsión de mejora objetivo A12
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de medio y alto a excelente para los controles con importancia alta o vital.

Tabla 27 Recomendaciones Objetivo A13

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	13.1.1 Controles de red	Documentar la responsabilidad de los técnicos de gestión de redes, su atribuciones y procesos asociados
	13.1.2 Seguridad de los servicios de red	Determinar las directrices de acceso y privilegios por usuario respecto a los servicios de comunicación, que incluya la responsabilidad y uso de la infraestructura de comunicaciones.
	13.1.3 Separación en las redes	Documentar el procedimiento de gestión de redes y sus dominios
	13.2.1 Políticas y procedimientos de transferencia de información	Documentar los procedimientos y protocolos de seguridad que garantizan la transferencia información a través de las redes de comunicación.
	13.2.2 Acuerdos de transferencia de información	Determinar la gestión de procedimientos criptográficos que aseguren las comunicaciones y protejan la información de afectaciones en la confidencialidad, integridad, disponibilidad y confiabilidad.
	13.2.3 Mensajería electrónica	Documentar las directrices respecto al uso de los servicios de mensajería electrónica institucional y la información transferida por estos medios
	13.2.4 Acuerdos de confidencialidad o no revelación	Establecer los acuerdos de confidencialidad respecto al uso de información institucional, la propiedad del activo, las sanciones por uso negligente o no autorizado inclusive al finalizar la relación contractual

Elaborado por: La Investigadora

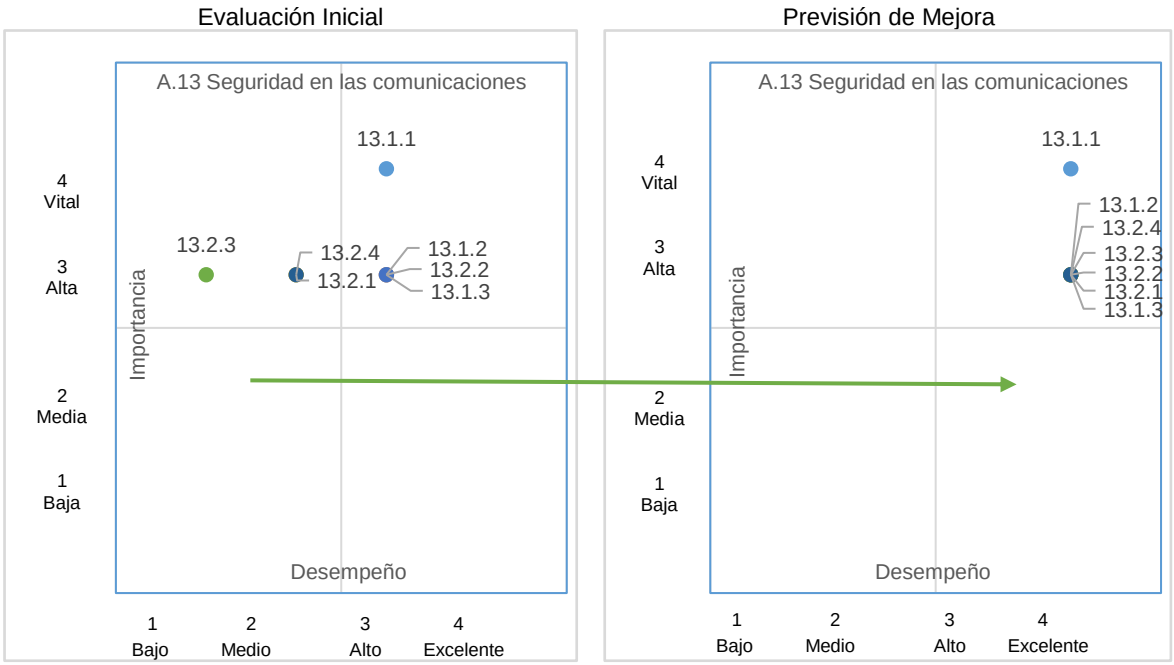


Gráfico 57 Comparación previsión de mejora objetivo A13
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de bajo, medio y alto a excelente para los controles con importancia alta o vital.

Tabla 28 Recomendaciones Objetivo A14

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Documentar los procedimientos de gestión de proyectos de desarrollo de software, incluyendo la gestión de la seguridad de la información, a lo largo de todos los procedimientos asociados.
	14.1.2 Asegurar los servicios de aplicaciones en redes públicas	Documentar los requisitos de seguridad que deben cumplir los sistemas en producción ya sean de uso interno o acceso web. Documentar los procedimientos de gestión de certificados digitales, responsables y ciclo de vida.
	14.1.3 Protección de las transacciones de servicios de aplicaciones	Documentar los procedimientos de gestión de certificados digitales, responsables y ciclo de vida.
	14.2.1 Política de desarrollo seguro 14.2.5 Principios de ingeniería de sistemas seguros 14.2.6 Ambiente de desarrollo seguro	Establecer directrices respecto a la utilización de principios de ingeniería de sistemas seguros que contemplen técnicas de autenticación, conexiones seguras, validación de datos, depuración de código, etc.

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	14.2.2 Procedimientos de control de cambios en sistemas	Se debe garantizar que las pruebas se ejecutan en ambientes separados a los de desarrollo y producción y la seguridad respecto a los datos de prueba utilizados, su acceso, manipulación y eliminado
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 14.2.4 Restricciones a los cambios en los paquetes de software	Documentar los procedimientos de pruebas y control de cambios que garanticen la usabilidad de los sistemas, previa su operación en producción, evaluando riesgos e impactos, control de versiones, actualización de manuales
	14.2.7 Desarrollo externalizado	El desarrollo externalizado debe cumplir las mismas características de seguridad que establece la gestión en seguridad para los proyectos de desarrollo
	14.2.8 Pruebas de seguridad del sistema 14.2.9 Pruebas de aceptación de sistemas	Determinar las directrices respecto a los procedimientos, validación y control de cambios para pruebas de seguridad y pruebas de aceptación
	14.3.1 Protección de los datos de prueba	Se debe garantizar que las pruebas se ejecutan en ambientes separados a los de desarrollo y producción y la seguridad respecto a los datos de prueba utilizados, su acceso, manipulación y eliminado.

Elaborado por: La Investigadora

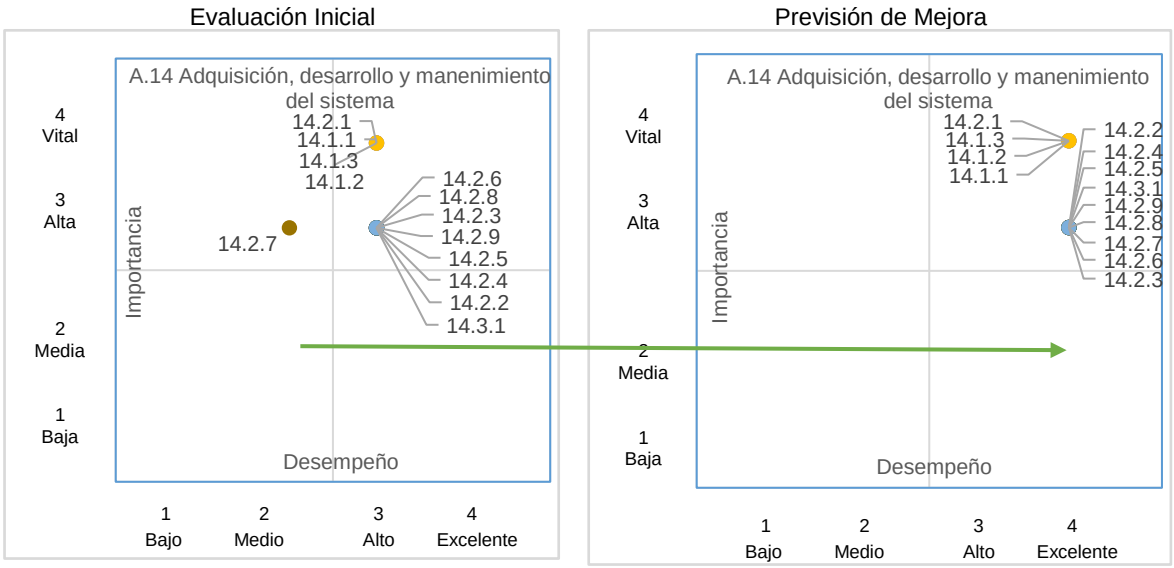


Gráfico 58 Comparación previsión de mejora objetivo A14
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de medio y alto a excelente para los controles con importancia alta o vital.

Tabla 29 Recomendaciones Objetivo A16

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Identificar y documentar los tipos de proveedores que requiere el giro del negocio, como: servicios de comunicación, equipamiento, consultoría, paquetes de software, de desarrollo, etc.
	15.1.2 Requisitos de seguridad en contratos con terceros	La documentación de soporte para los procesos de contratación debe contemplar los requisitos de seguridad esperados sobre los productos o servicios, como actualización tecnológica, cumplimiento de estándares, garantía, soporte, mantenimiento, etc.
	15.1.3 Cadena de suministro de tecnologías de la información y de las comunicaciones	Dentro de la relación de con proveedores se debe considerar los acuerdos de confidencialidad y uso de información, cuando la relación contractual así lo requiera.
	15.2.1 Monitoreo y revisión de los servicios de proveedores. 15.2.2 Gestión de cambios en los servicios de proveedores.	Se debe documentar los requisitos de seguridad que deben cumplir los productos o servicios que son contratados a terceros.

Elaborado por: La Investigadora

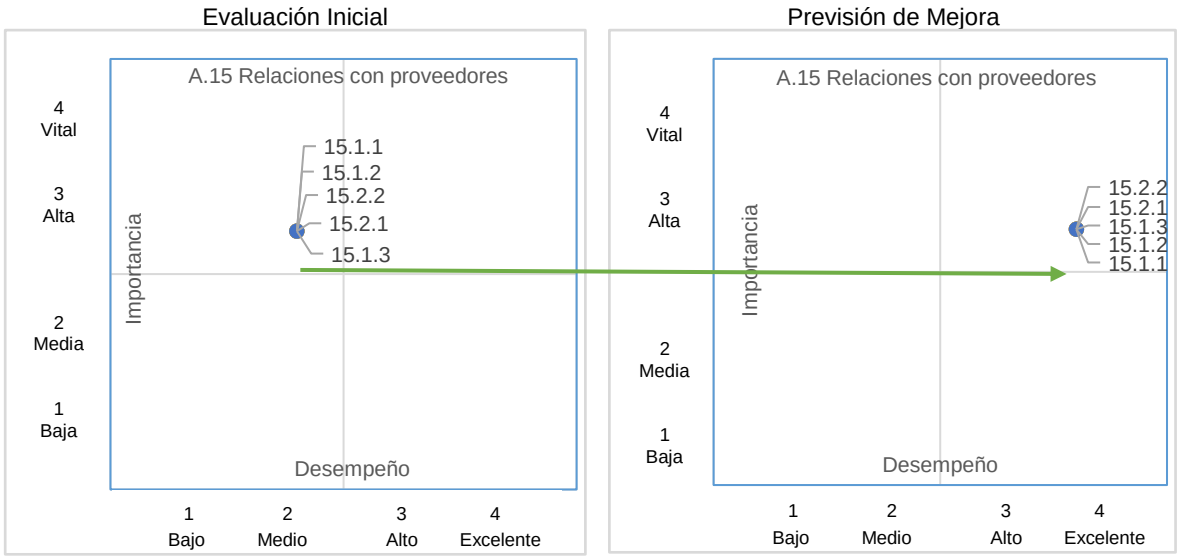


Gráfico 59 Comparación previsión de mejora Objetivo A15
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de medio a excelente para los controles con importancia alta o vital.

Tabla 30 Recomendaciones Objetivo A16

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	16.1.1 Responsabilidades y procedimientos	Determinar las regulaciones respecto a la gestión de incidentes de seguridad que contemple: planificación, evaluación y toma de decisiones. Las regulaciones deben contemplar la necesidad de Documentar los incidentes de seguridad para su monitoreo, aprendizaje y retroalimentación. Se debe Establecer formatos homologados que permitan Documentar lo incidentes de seguridad.
	16.1.2 Informe de los eventos de seguridad de la información	Establecer el canal de comunicación y periodicidad para notificar los incidentes de seguridad al nivel jerárquico superior y estratégico conforme la criticidad de los eventos suscitados.
	16.1.3 Informe de debilidades de seguridad de la información	La notificación de eventos de seguridad debe incluir al personal, quienes deben tener la responsabilidad de anotar y notificar cualquier debilidad o falla de seguridad que se identifique respecto a los sistemas
	16.1.4 Apreciación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad deben ser clasificados por su criticidad para evaluar los que requieran ser notificados, como, por ejemplo: inseguridad en las comunicaciones, afectación a la confidencialidad, integridad o disponibilidad, negligencia, incumplimiento de directrices, falla de software o hardware, accesos no autorizados, etc.
	16.1.5 Respuesta a incidentes de seguridad de la información 16.1.6 Aprendizaje de los incidentes de seguridad de la información 16.1.7 Recopilación de evidencias	Que recupere la fiabilidad respecto a la seguridad de la información y que considere: recolección de evidencias, análisis forense, escalado de incidentes, tratamiento de la debilidad y cierre del incidente. Todo esto de forma documentada para su posterior análisis y reducción de posibilidades de futuras ocurrencias.

Elaborado por: La Investigadora

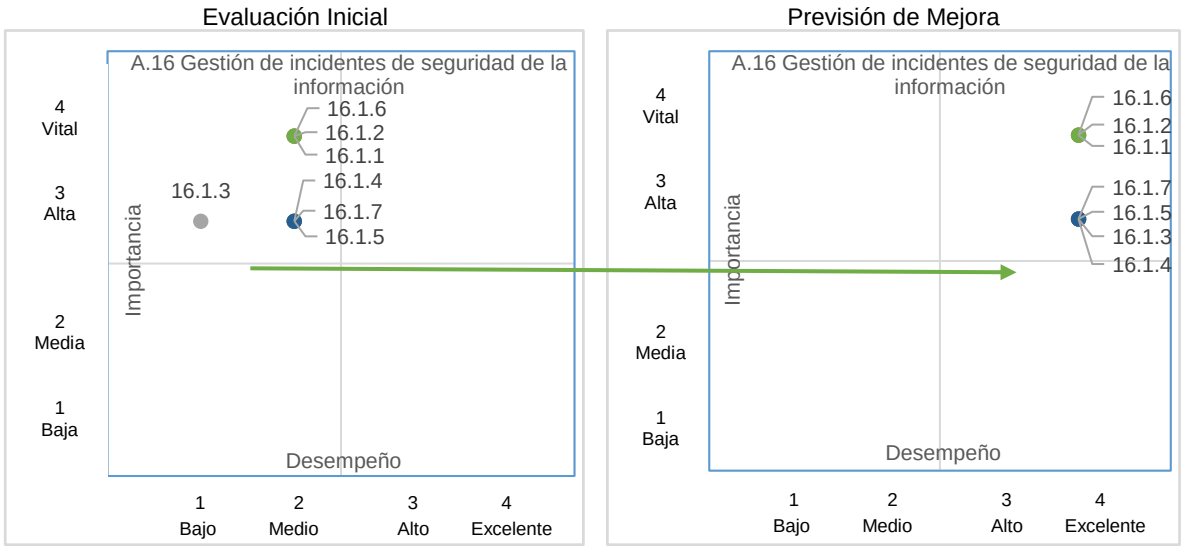


Gráfico 60 Comparación previsión de mejora objetivo A16

Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de bajo y medio a excelente para los controles con importancia alta o vital.

Tabla 31 Recomendaciones Objetivo A17

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	17.1.1 Planificación de la continuidad de seguridad de la información 17.1.2 Implementación de la continuidad de seguridad de la información 17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información	Para un adecuado monitoreo es necesario se proyecte la ejecución de planes de: supervisión a las actividades de los administradores, mantenimiento de infraestructura hardware, sistemas, redes de comunicación, gestión de riesgos, capacitación y actualización de controles y políticas de seguridad.
	17.2.1 Disponibilidad de las instalaciones de procesamiento de la información	Documentar los controles de seguridad implementados

Elaborado por: La Investigadora

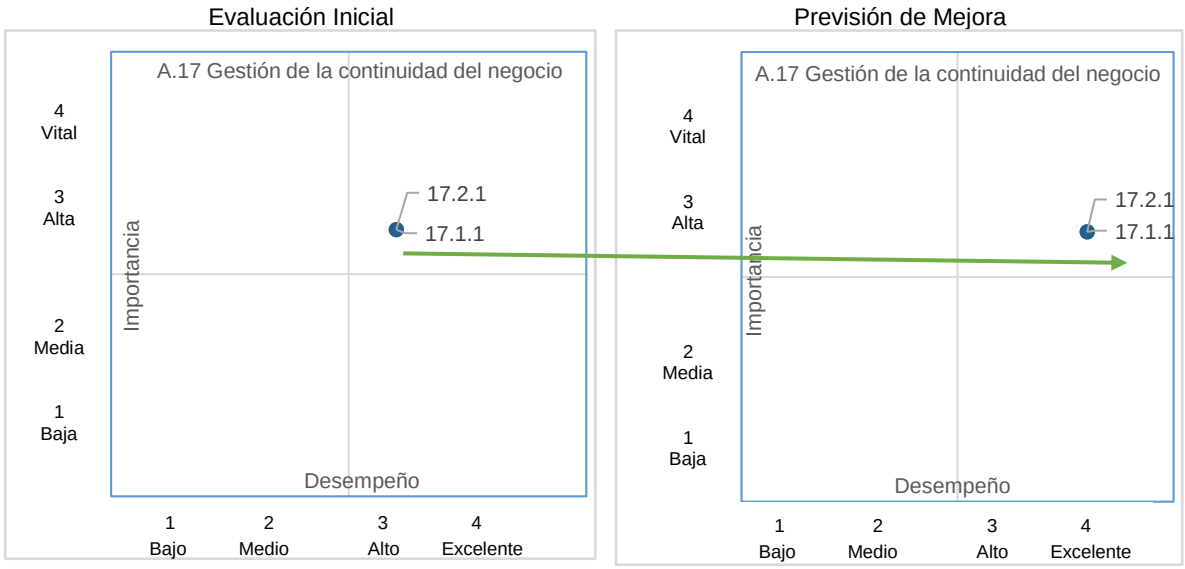


Gráfico 61 Comparación previsión de mejora objetivo A17
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de alto a excelente para los controles con importancia alta o vital.

Tabla 32 Recomendaciones Objetivo A18

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Documentar la normativa legal que rige la operación institucional
	18.1.2 Derechos de propiedad intelectual 18.1.3 Protección de los registros 18.1.4 Protección y privacidad de la información de carácter personal	Toda acción orientada a la gestión de la seguridad de la información debe partir desde las leyes, reglamentos y disposiciones externas e internas que son de cumplimiento obligatorio para la institución. En este contexto, se deberá considerar necesariamente las directrices de protección de propiedad intelectual y de confidencialidad de la información personal
	18.1.5 Reglamentos de controles criptográficos	Documentar el procedimiento de aplicación de controles criptográficos, responsables, vigencia y monitoreo
	18.2.1 Revisión independiente de seguridad de la información	El nivel directivo es responsable del monitoreo y continuidad de la seguridad

Objetivo de Control	Control	Recomendaciones conforme la gestión de seguridad
	18.2.2 Cumplimiento de las políticas y normas de seguridad	El monitoreo y evaluación de resultados obtenidos debe ser utilizado para analizar la gestión de la seguridad de la información en un período determinado de tiempo. El resultado de este análisis debe permitir tomar las decisiones adecuadas respecto a cómo se manejará la continuidad de la seguridad
	18.2.3 Comprobación del cumplimiento técnico	Determinar la responsabilidad de supervisión de vulnerabilidades técnicas en cumplimiento de las actualizaciones de seguridad disponibles.

Elaborado por: La Investigadora

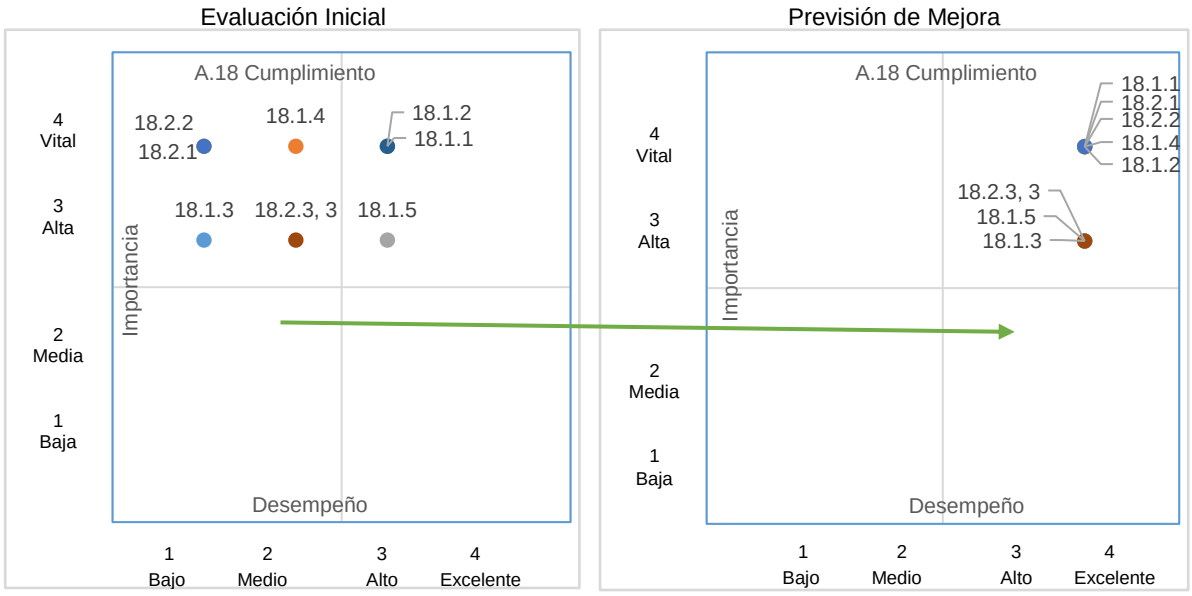


Gráfico 62 Comparación previsión de mejora objetivo A18
Elaborado por: La Investigadora

La gestión de seguridad de la información prevé mejorar el desempeño de bajo, medio y alto a excelente para los controles con importancia alta o vital.

6.10 Análisis e interpretación de resultados

Las previsiones antes citadas, se complementan con la aplicación de una segunda encuesta a los usuarios del sistema académico de la UNACH, que permita evaluar la efectividad de la propuesta desarrollada, para la cual se empleó la misma población y muestra de la investigación, así:

- Personal de la Unidad Técnica de Control Académico: 3 (población total)
- Administrador de la Red Institucional: 1 (población total)
- Operadores del sistema académico: 51 (población total)
- Estudiantes: 95 (muestra aleatoria)
- Docentes: 82 (muestra aleatoria)

1. **¿Considera usted que la metodología propuesta para la identificación y valoración de activos, su monitoreo, tratamiento y mejora, permite gestionar la seguridad respecto a los activos de información del sistema académico?**

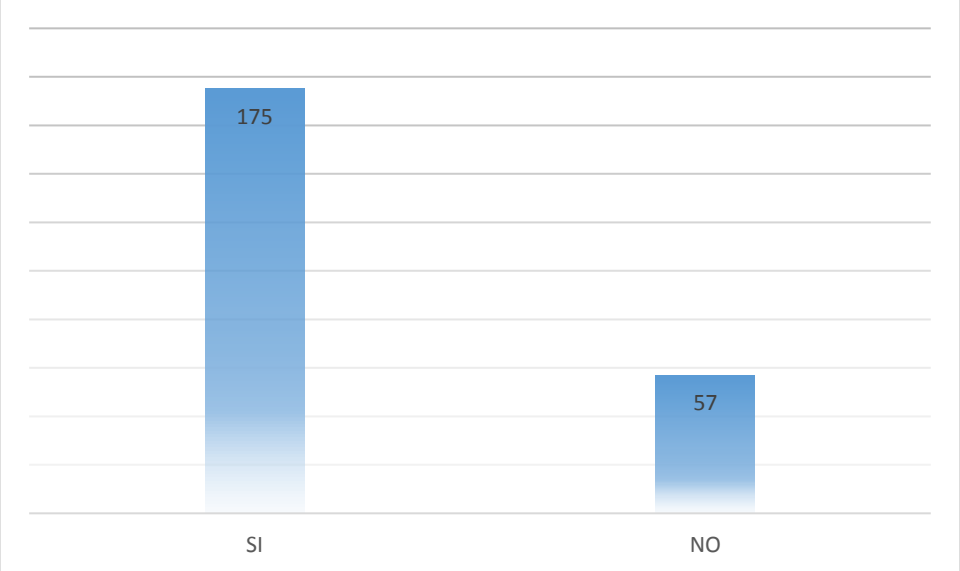


Gráfico 63 Pregunta respecto a la Sección I de la Propuesta: Gestión de Activos
Elaborado por: La Investigadora

Análisis: 175 encuestados equivalente al 75,43% considera que la metodología propuesta para la identificación y valoración de activos si permite gestionar la seguridad respecto a los activos de información, mientras 57 encuestados equivalente que un 24,57% manifiesta que no.

Interpretación: Los resultados obtenidos permiten concluir que el 75,43% de usuarios considera efectiva la propuesta respecto a la Gestión de Activos de Información.

2. **¿Considera usted que la propuesta respecto al marco regulatorio para la seguridad de la información que abarque no solo el cumplimiento de la norma vigente, sino que establezca políticas respecto a la organización interna, recursos humanos, activos de información, gestión de proyectos y manejo de incidentes, contribuye a una adecuada gestión de la seguridad de la información en el sistema académico?**

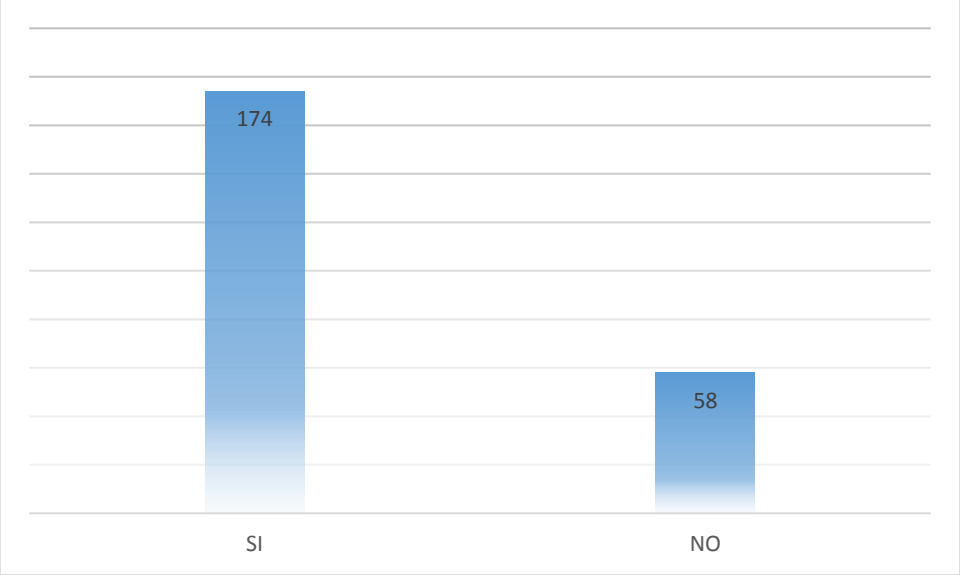


Gráfico 64 Pregunta respecto a la Sección II de la Propuesta: Marco Regulatorio
Elaborado por: La Investigadora

Análisis: 174 encuestados equivalente al 75% considera que la propuesta respecto al marco regulatorio que debe ser implementado SI contribuye a la

gestión de la seguridad de la información, mientras 58 encuestados equivalente al 25% manifiesta que no.

Interpretación: Los resultados obtenidos permiten concluir que el 75% de usuarios considera efectiva la propuesta respecto a las Regulaciones.

3. **¿Considera usted que la propuesta respecto a la necesidad de contar un plan de gestión de incidentes que asegure los responsables, acciones y respuestas ante tales eventos; incide en la seguridad de la información en el sistema académico?**

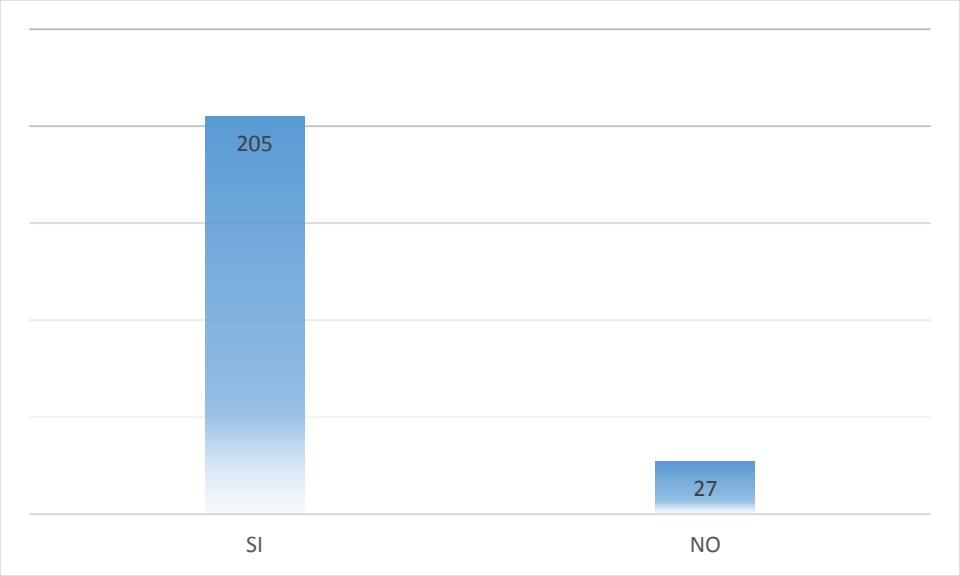


Gráfico 65 Pregunta respecto a la Sección III de la Propuesta: Gestión de Incidentes
Elaborado por: La Investigadora

Análisis: 205 encuestados equivalente al 88,36% considera que la propuesta respecto a la necesidad de contar con un plan de gestión de incidentes SI incide en la seguridad de la información del sistema académico, mientras 27 encuestados equivalente que un 11,64% manifiesta que no.

Interpretación: Los resultados obtenidos permiten concluir que el 88,36% de usuarios considera efectiva la propuesta respecto a la Gestión de Incidentes de seguridad.

4. **¿Considera que la seguridad de la información del sistema académico debe ser apoyada mediante un plan de monitoreo y continuidad, que considere las responsabilidades del personal, planes de mantenimiento, capacitación, actualización de controles de seguridad y revisión de políticas de seguridad, conforme la propuesta?**

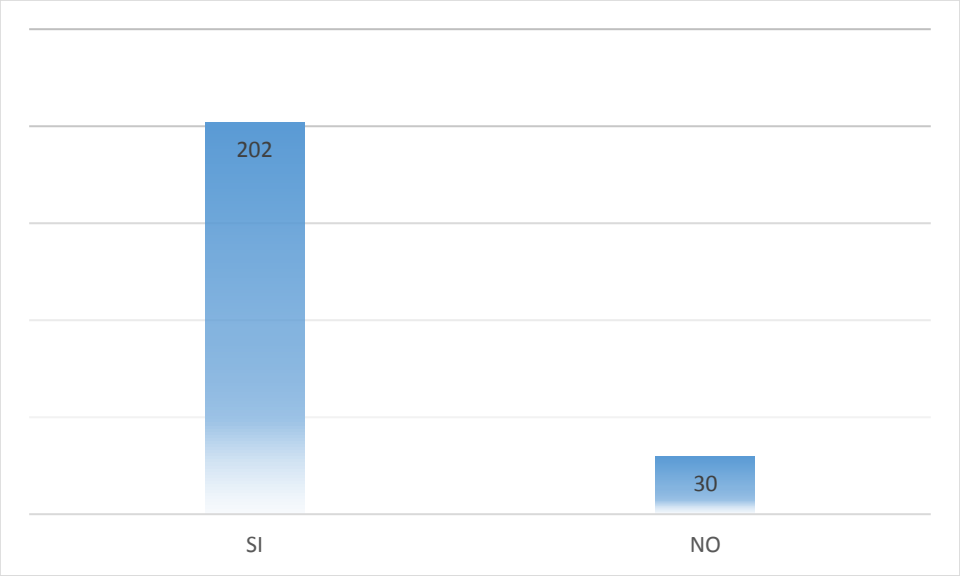


Gráfico 66 Pregunta respecto a la Sección IV de la Propuesta: Monitoreo y Continuidad
Elaborado por: La Investigadora

Análisis: 20 encuestados equivalente al 87,07% considera que la seguridad de la información, SI debe ser apoyada con un plan de monitoreo y continuidad conforme la propuesta de seguridad de la información, mientras 30 encuestados equivalente que un 11,93% manifiesta que no.

Interpretación: Los resultados obtenidos permiten concluir que el 87,07% de usuarios considera efectiva la propuesta respecto al Monitoreo y Continuidad de la Seguridad de la Información.

Para corroborar la información previa de comprobación de la hipótesis, se utilizó nuevamente el método estadístico X^2 (Ji- Cuadrado), con los parámetros ya considerados, obteniendo los siguientes resultados:

Cálculos:

Frecuencia Observada

Tabla 33 Frecuencia Observada fo – Encuesta respecto a la efectiva de la propuesta

Pregunta	SI	NO	Total
Pregunta 1. ¿Considera usted que la metodología propuesta para la identificación y valoración de activos, su monitoreo, tratamiento y mejora, permite gestionar la seguridad respecto a los activos de información del sistema académico?	175	57	232
Pregunta 2. ¿Considera usted que la propuesta respecto al marco regulatorio para la seguridad de la información que abarque no solo el cumplimiento de la norma vigente, sino que establezca políticas respecto a la organización interna, recursos humanos, activos de información, gestión de proyectos y manejo de incidentes, contribuye a una adecuada gestión de la seguridad de la información en el sistema académico?	174	58	232
Pregunta 3. ¿Considera usted que la propuesta respecto a la necesidad de contar un plan de gestión de incidentes que asegure los responsables, acciones y respuestas ante tales eventos; incide en la seguridad de la información en el sistema académico?	205	27	232

Pregunta 4. ¿Considera que la seguridad de la información del sistema académico debe ser apoyada mediante un plan de monitoreo y continuidad, que considere las responsabilidades del personal, planes de mantenimiento, capacitación, actualización de controles de seguridad y revisión de políticas de seguridad, conforme la propuesta?	202	30	232
Total	756	172	928

Fuente: *Encuesta usuarios*
Elaborado por: La Investigadora

Prueba de la hipótesis

Tabla 34 Prueba de la Hipótesis

Pregunta	**SI**		**NO**		**$(fo-fe)^2$ /fe**
	fo	**fe**	**fo**	**fe**	
1	175	189	57	43	1.04
2	174	189	58	43	1.19
3	205	189	27	43	1.35
4	202	189	30	43	0.89
X^2 Ji - Cuadrado					**4.48**

Elaborado por: La Investigadora

Criterio:

Se rechaza la hipótesis nula si $X^2 < \alpha$

Valores X^2 para 52 grados de Libertad					
	Probabilidad de un valor superior a α				
	0,01	**0,05**	0,10	0,20	0,25
52	21.67	**8.34**	14.68	12.24	11.39

Obtenido el resultado de X^2 4.48 < 8.34, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis de investigación (Hi), esto es: Las normas ISO 27001 y 27002 SI inciden en la seguridad de la información.

Conclusiones:

- Las Instituciones de Educación Superior deben contar con procesos formalmente establecidos para la gestión en seguridad de la información, que permitan preservar la confidencialidad, integridad y disponibilidad de la misma.
- De las IES analizadas se puede observar que una ha alcanzado el nivel 4 de madurez (certificación bajo un estándar de buenas prácticas en seguridad), encontrándose las demás en nivel 1 (Implantación de medidas básica) o nivel 2 (adaptación a requisitos legales), lo cual evidencia que no existe una adecuada seguridad de la información contenida en sus bases de datos.
- La gestión en seguridad de la información planteada para la UNACH con base a la aplicación de las normas 27001 y 27002, pretende que se alcance el nivel 3 de madurez (definición de políticas, procedimientos, análisis y gestión de riesgos, plan de atención de incidentes y continuidad del negocio).
- Lo expuesto permite ratificar que la aplicación de un marco normativo, metodológico y sistemático respecto a la seguridad de la información, como en este caso las normas ISO 27001 y 27002, si incide en la seguridad de los datos, su monitoreo, tratamiento y mejora.
- El marco normativo citado, robustece la seguridad de las bases de datos, por lo que, la confidencialidad, integridad y disponibilidad de la información pueden ser garantizadas en los diferentes procesos institucionales,

Recomendaciones:

A la Universidad Nacional de Chimborazo para que implemente la gestión de activos de información, que permite su identificación, evaluación y monitoreo, facilitando la detección de vulnerabilidades y prevención de riesgos de seguridad.

A la Universidad Nacional de Chimborazo para que se norme el proceso de gestión de seguridad, estableciendo políticas de obligatorio cumplimiento para los usuarios.

A la Universidad Nacional de Chimborazo, para que implemente la propuesta de gestión de seguridad de la información, que permita un adecuado trabajo respecto a sus activos de información, orientando esfuerzos para que la confidencialidad, integridad y disponibilidad no se vean afectadas por incidentes de seguridad con o sin la intención de provocar daño.

BIBLIOGRAFÍA

- AGUIRRE F, PALACIOS J. (2014). *Evaluación técnica de seguridades del Data Center del Municipio de Quito según las normas ISO/IEC 27001:2005 SGSIE ISO/IEC 27002:2005*. Recuperado de https://repositorio.espe.edu.ec/bitstream/21000/8303/1/T-ESPE-047892.pdf
- ASAMBLEA CONSTITUYENTE. (sf). *Constitución del Ecuador.* Recuperado de http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf
- ASAMBLEA CONSTITUYENTE. (2010). *Ley del Sistema Nacional de Registro de Datos Públicos*. Recuperado de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/LEY-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf
- BIONEL, A. (2013). *Matriz "Importance Performance Analysis" de atributos críticos de satisfacción de alumnos en ciencia y tecnología y medidas correctivas frente a la meta-acreditación institucional.* Recuperado de http://www.palermo.edu/ingenieria/pdf2014/13/CyT_13_01.pdf
- CONTRALORÍA GENERAL DEL ESTADO. (2009). *Normas de Control Interno de la Contraloría General del Estado.* Recuperado de http://www.gobiernoelectronico.gob.ec/wp-content/uploads/downloads/2017/09/Normas-de-control-interno-de-la-CGE.pdf
- DRAE. (2017). *Diccionario de la Real Academia Española*. Recuperado de http://dle.rae.es/?id=LXrOqrN
- ECHENIQUE, J. (2001). *Auditoría en Informática*. México D.F. México. McGraw-Hill.
- EL COMERCIO. (2015). *Cibermafias atacaron a 17 empresas ecuatorianas.* Recuperado de

http://www.elcomercio.com/actualidad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html

- EL PAÍS. (2013). *Investigan millonario robo con claves del municipio en Riobamba, Ecuador.* Recuperado de http://www.elpais.com.co/mundo/investigan-millonario-robo-con-claves-del-municipio-en-riobamba-ecuador.html
- EL TELÉGRAFO. (2011). *Ataques hacker a redes de Ecuador.* Recuperado de http://www.eltelegrafo.com.ec/noticias/tecnologia/30/mas-paginas-web-oficiales-hackeadas
- EL TELÉGRAFO. (2016). *En Ecuador, el 85% de los delitos informáticos ocurren por descuido del usuario.* Recuperado de https://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario
- GÓMEZ, A. (2011). Enciclopedia de la Seguridad Informática. México D.F. México. Alfaomega.
- INEN (2017). *Tecnologías dela información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Requisitos (ISO/IEC 27002: 2013 + Cor. 1:2014. 2:2015, IDT)*. Quito. Ecuador: INEN.
- INEN (2017). *Tecnologías de la información. Técnicas de seguridad. Código de práctica para los controles de seguridad de la información (ISO/IEC 27002: 2013 + Cor. 1:2014. 2:2015, IDT).* ISO/EC 27001:2013. Quito. Ecuador: INEN.
- INEN (2011). *Tecnologías dela información. Técnicas de seguridad – Gestión del Riesgo en la Seguridad de la Información. NTE INEN ISO/IEC 27005:2012. Quito. Ecuador. INEN.*
- ISO. (s/f). *Software ISO Riesgos y Seguridad.* Recuperado de https://www.iso.org/standard/54534.html
- LA HORA: (2013). *Robo en Municipio de Riobamba se dio por mal uso de claves, según BCE.* Recuperado de https://lahora.com.ec/noticia/1101493206/robo-en--municipio-de-riobamba-se-dio-por-mal-uso-de-claves-segc3ban-bce

- LANCHE, D (2015). *Diseño de un sistema de seguridad de la información para la compañía COTECNIC Cia. Ltda. basado en la norma NTE INEN ISO /IEC 27002*. Recuperado de http://dspace.uazuay.edu.ec/bitstream/datos/3585/1/10269.pdf
- LAUDON, K (2010). *Sistemas de información: fundamentos y análisis*. México D.F. México. Pearson Educación
- LEXIS. (sf). *Ley Orgánica de Transparencia y Acceso a la Información Pública*. Recuperado de http://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cpccs_22_ley_org_tran_acc_inf_pub.pdf
- LEXIS. (sf). *Ley de Comercio Electrónico, firmas y mensajes de datos*. Recuperado de http://www.oas.org/juridico/pdfs/mesicic4_ecu_comer.pdf
- MANTILLA A y NARANJO J, (2009). *Diseño de un sistema de gestión de seguridad de la información para cooperativas de ahorro y crédito en base a la norma ISO 27001*. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/8108/1/CD-2254.pdf
- MAPCAL. (1990). *Instrumentos de análisis de Marketing Estratégico.* Madrid. España. Ediciones Díaz de Santos S.A.
- PIATTINI, M. DEL PESO, E y DEL PESO M. (2008). *Auditorías de Tecnologías y Sistemas de Información*. México D.F. México. Alfaomega Grupo Editor, S.A. de C.V
- UNACH. (2009). Reglamento del Centro de Cómputo. Recuperado de http://www.unach.edu.ec/reglamentos/images/pdf/reglamentos/bloque_lale_2/reglamento_centro_de_computo.PDF
- SILBERSCHATZ, A., KORTH, H. SUDARSHAN, S. (2006). *Fundamentos de Bases de Datos.* Madrid. McGraw-Hill Interamericana
- TIXILIMA, V. (2015). *Elaboración de políticas y normas de seguridad de la información en base a la norma de seguridad ISO/IEC 27001, y el análisis de riesgos realizado aplicando la metodología Magerit y la herramienta Pilar.* Recuperado de: http://repositorio.puce.edu.ec/handle/22000/11437

- TOLA, D (2015). *Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO /IEC 27001*. Recuperado de https://www.dspace.espol.edu.ec/retrieve/89073/D-84631.pdf
- TORRES, H. (2010). *Diseño de la seguridad informática en la implementación de data center de la Universidad Nacional de Loja.* Recuperado de http://dspace.ucuenca.edu.ec/handle/123456789/2535
- UNIVERSIDAD DE COLIMA. (2017). *Sistema de Gestión de Seguridad de la Información. Sitio Oficial.* Recuperado de http://www1.ucol.mx/iso/iso27001

ANEXOS

Auditoría de seguridad de la información respecto a las bases de datos del sistema académico de la Universidad Nacional de Chimborazo, con base a la norma NTE INEN-ISO/IEC 27001 y 27002

I. Antecedentes

La auditoría surge de la necesidad de determinar si existe una incidencia de la aplicación de las normas ISO 27001 y 27002 en la seguridad de las bases de datos del sistema académico de la Universidad Nacional de Chimborazo.

II. Objetivo de la auditoría

Analizar la seguridad de la información de las bases de datos del sistema académico conforme las normas NTE INEN-ISO/IEC 27001 y 27002

III. Alcance y Metodología

Evaluar las áreas y procesos que estén en directa relación con el acceso, registro, manipulación y eliminación de información de las bases de datos, aplicando las normas NTE INEN-ISO/IEC 27001 y 27002, así:

Tabla 35 Alcance - Metodología Auditoría Seguridad de la Información UNACH

No	Alcance – Objetivo de Control	Metodología/ Requisitos
1	A5. Políticas de seguridad de la información	Entrevista Encuesta
2	A6. Organización de seguridad de la información	Entrevista Encuesta Revisión de responsabilidades y roles para acceso a la información Análisis de definición de bases de datos (diccionario de datos, DDL, DML)

No	Alcance – Objetivo de Control	Metodología/ Requisitos
		Integridad de Bases de Datos
3	A7. Seguridad en recursos humanos	Entrevista Encuesta Revisión de políticas e información documental respecto a divulgación de información, relación contractual y responsabilidades
4	A8. Gestión de activos	Entrevista Encuesta Activos de información
5	A9. Control de acceso	Entrevista Encuesta Capacitación a usuarios Pruebas de inicio de sesión Control de cambios Disponibilidad
6	A10.Criptografía	Entrevista Encuesta
7	A11. Seguridad física y del entorno	Entrevista Encuesta
8	A12. Equipos	Entrevista Encuesta Revisión de información documental (plan de mantenimiento de equipos, autorización de salida de equipos, procedimientos de operación) Cumplimiento de estándares de seguridad Control actividades de usuarios, administradores y fallos Análisis de vulnerabilidades técnicas
9	A13. Seguridad en las comunicaciones	Entrevista Encuesta Análisis de controles implementados Pruebas de vulnerabilidad en las comunicaciones
10	A14. Adquisición, desarrollo y mantenimiento del sistema	Entrevista Encuesta Revisión información documental (guías, manuales)

No	Alcance – Objetivo de Control	Metodología/ Requisitos
11	A15. Relación con proveedores	Entrevista Encuesta Revisión información documental
12	A16. Gestión de incidentes de seguridad de la información	Entrevista Encuesta Revisión información documental
13	A17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Entrevista Encuesta Revisión información documental
14	A18. Cumplimiento	Entrevista Encuesta Revisión información documental

Fuente: Plan de Auditoría preparado por la Investigadora
Elaborado por: La Investigadora

Es importante señalar que la información de carácter sensible como redes, configuraciones, permisos, servicios y aplicaciones no han sido detallados en este documento, por procedimiento de seguridad y restricciones emitidas por parte de la institución; por lo que, los resultados se expresan de manera global.

IV. Tiempo de ejecución

La auditoría se cumplió en un plazo de 18 semanas, conforme el siguiente cronograma.

Tabla 36 Cronograma Auditoría - UNACH

No	Fase	Tiempo en semanas
1	Planeación del proceso de auditoría	3 semanas
2	Solicitud de información documental	2 semana
3	Aplicación de encuestas y entrevistas	2 semana
3	Observación directa	2 semanas
4	Ejecución de pruebas de vulnerabilidad	3 semanas
5	Procesamiento de información recibida	3 semanas
6	Análisis e interpretación de resultados	2 semana

7	Elaboración de informe	1 semana
TOTAL		**18 semanas**

Elaborado por: La Investigadora

V. Evaluación de la información

Se utilizó conforme el plan de auditoría la matriz de evaluación del nivel de madurez de los controles de seguridad, de acuerdo a los resultados obtenidos de las encuestas, entrevistas, observaciones y revisión documental realizadas; siendo dicha evaluación de tipo cuantitativa respecto al nivel de madurez de cada uno de los controles, de acuerdo a las siguientes escalas:

Tabla 37. Escala para evaluar el nivel de madurez respecto al control de seguridad

Puntuación	Equivalencia	Interpretación
1	Bajo	Inexistente. No existe información documentada o no se ha implementado el control.
2	Medio	Etapa 1 de madurez. Se han implementado esfuerzos puntuales, pero no de forma documentada o sistemática.
3	Alto	Etapa 2 de madurez. Se cuenta con evidencia documental o el proceso informal ya es repetitivo. Depende mucho del conocimiento de las personas. Cumple la normativa legal que rige el giro del negocio.
4	Excelente	Etapa 3 de madurez. Está implementado un control documentado respecto a la seguridad de la información, su monitoreo, tratamiento y mejora.

Fuente: Matriz de evaluación nivel de madurez controles de seguridad
Elaborado por: La Investigadora

VI. Pruebas de controles

Para complementar los resultados de la evaluación de seguridad de la información, se realizó la verificación de controles implementados y pruebas de vulnerabilidad, a fin de determinar posibles riesgos a los que esté expuesta la información de los SGBD.

A nivel local se analizó las configuraciones de bases de datos (sin autorización de captura de pantalla) y desde exterior se realizó pruebas de vulnerabilidad (capturas de pantalla con pixelación deliberada por protección de información) utilizando Nessus y Zed Attack Proxy (ZAP), cuyos principales resultados fueron los siguientes:

Tabla 38 Matriz pruebas de seguridad

No	Tipo	Prueba /Revisión	Resultado
1	Local. Base de Datos	Registro de transacciones. Datos de entrada (fecha, hora, usuario)	Registro SQL a nivel de transacciones. Gráfico 63.
2	Local. Red	Monitoreo red de comunicaciones	Utilización de software de monitoreo Cacti y Nagios. Gráfico 64.
3	Local. Base de datos	Store procedures Funciones Particionamiento	Procedimientos almacenados y funciones para validación de datos, control de operaciones, etc. Particionamiento físico y lógico para rendimiento y velocidad en el acceso a los datos. Adecuada utilización de procedimientos y funciones.
4	Local. Base de datos	Verificación de registros	No se realiza un monitoreo de registros
5	Local. Base de datos	Integridad de Base de datos	Integridad referencial, de dominio e integral
6	Local. Base de datos	Roles y permisos	Rol de nivel de servidor para el Administrador. Roles por entidad para usuarios.
6	Local. Aplicación	Aceptación de usuarios finales de transacciones	Confirmación de datos a modificar previo registro
7	Local. Red	Escaneo Básico	9 vulnerabilidades de riesgo medio. Requiere actualización de controles. Gráfico 65.
8	Exterior. Aplicación	Registro e ingreso de usuarios	Riesgo medio: Clickjacking. Riesgo medio: XSS reflejado Riesgo bajo: Ataque de diccionario Riesgo medio: SQL Injection. Gráficos 66, 67.

No	Tipo	Prueba /Revisión	Resultado
9	Exterior. Aplicación	Recuperación datos de usuario	Valida historial de contraseñas. Valida cantidad de caracteres admitidos. No admite caracteres especiales. No advierte al usuario. Se identificó en prueba de recuperación de contraseña. Gráfico 68.
10	Exterior. Aplicación	Aplicación web	2 vulnerabilidades de riesgo medio. Requiere actualización de controles. Gráfico 69.

Fuente: Pruebas de vulnerabilidad realizadas
Elaborado por: La Investigadora

	MatriculaID	EstudianteID	FechaEmision	FechaLegalizacion	Situacion	FacturaPago	OrdenID	UsuarioID	FechaTransaccion
1	96	1001	2004-10-19 10:24:35.747	2004-10-19 10:27:54.093	LEGALIZADA	0023019	2	15	2004-10-19 10:27:54.093
2	97	1002	2004-10-19 10:51:33.653	2004-10-19 10:52:32.513	LEGALIZADA	0024041	3	15	2004-10-19 10:52:32.513
3	98	1003	2004-10-19 11:21:47.483	2004-10-19 11:22:53.903	LEGALIZADA	0021155	5	15	2004-10-19 11:22:53.903
4	99	1005	2004-11-08 11:51:55.357	2004-11-08 11:53:02.513	LEGALIZADA	21273	8	15	2004-11-08 11:53:02.513
5	100	1006	2004-11-10 16:34:14.763	2004-11-10 16:51:18.937	LEGALIZADA	24455	10	15	2004-11-10 16:51:18.937
6	101	1010	2004-11-10 18:17:36.263	2005-06-24 08:26:36.890	LEGALIZADA	22844	13	15	2005-06-24 08:26:36.890
7	102	1008	2004-11-10 18:26:04.577	2004-11-10 18:28:07.983	LEGALIZADA	18526	15	15	2004-11-10 18:28:07.983
8	103	1007	2004-11-10 19:08:45.547	2005-06-23 14:52:38.560	LEGALIZADA	23493	16	15	2005-06-23 14:52:38.560
9	104	1011	2004-11-12 11:00:23.357	2005-06-24 08:43:11.263	LEGALIZADA	20706	18	15	2005-06-24 08:43:11.263

Gráfico 67 Registro Transacciones por Usuario - Base de Datos
Recuperado de: Base de datos sistema académico

(Pixelación deliberada por seguridad de información de la red)

Gráfico 68 Monitoreo Cacti a la red de comunicaciones - registro de transacciones
Recuperado de: Cacti – monitoreo red de comunicaciones

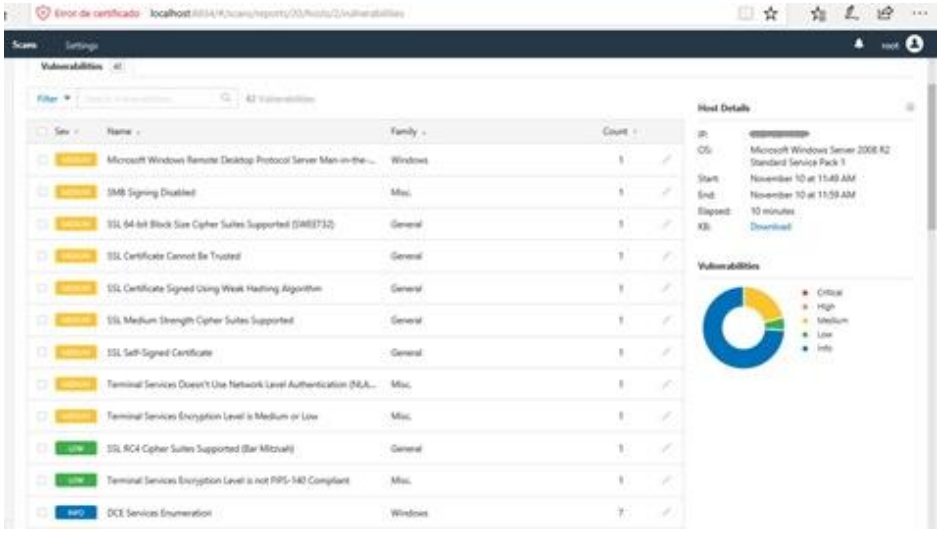


Gráfico 69 Escaneo Básico red local
Recuperado de: Nessus

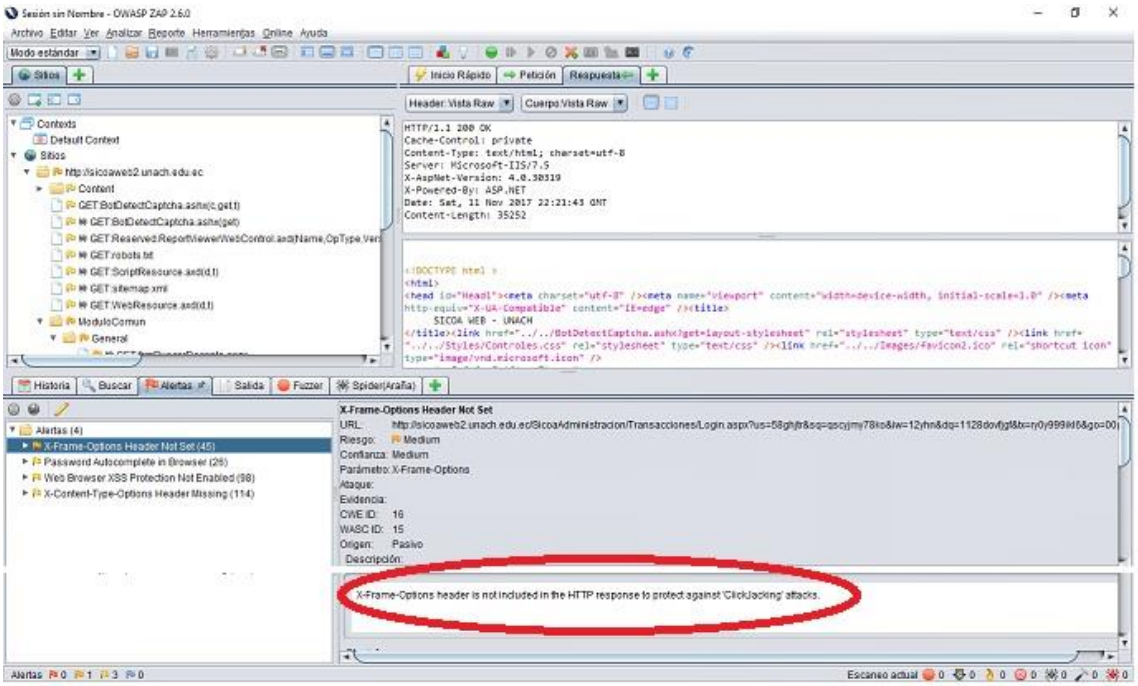


Gráfico 70 Prueba de vulnerabilidad aplicación web
Recuperado de: OWASP ZAP

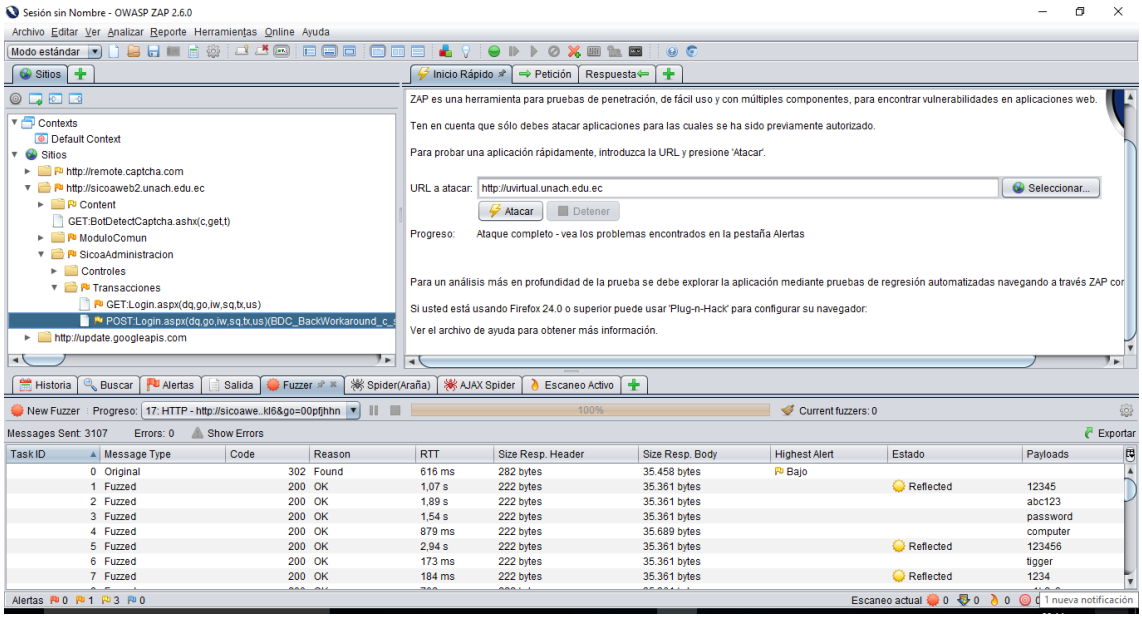


Gráfico 71 Prueba de vulnerabilidad ataque de diccionario
Recuperado de: OWAP ZAP

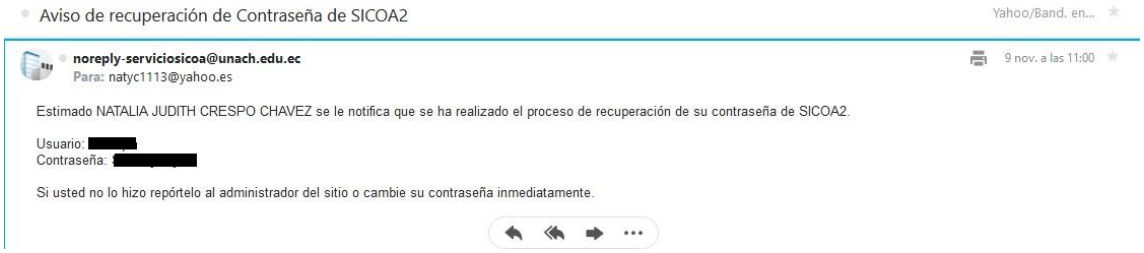


Gráfico 72 Recuperación datos usuario – acceso sistema académico
Recuperado de: SICOA2

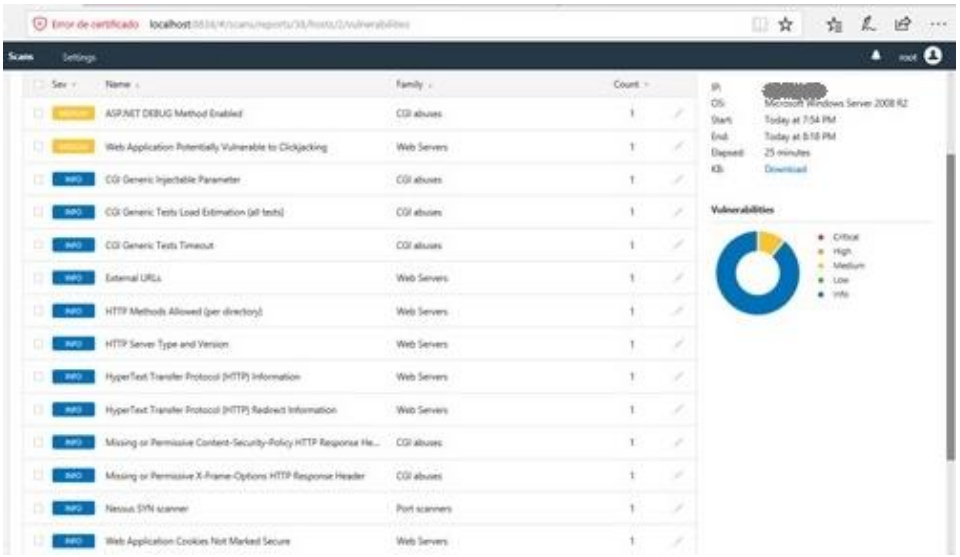


Gráfico 73 Escaneo Básico IP Pública
Recuperado de: Nessus

VII. Informe

Para el análisis de madurez se consideró los 14 objetivos y 114 controles de seguridad que establecen las normas 27001 y 27002, determinando el mismo en función del resultado obtenido (estado actual del control en la unidad evaluada), respecto a lo que establece la norma.

De la evaluación del nivel de madurez y las pruebas de vulnerabilidad realizadas se obtienen los siguientes resultados, así:

Tabla 39 Matriz de evaluación nivel de madurez de los controles de seguridad

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
A5. Política de seguridad de la información					
1	5.1.1 Política de seguridad de la información para los SGBD	Política aprobada, implementada, socializada (número de eventos, concienciación a usuarios) y disponible (publicada en un lugar de fácil acceso para todos los usuarios), que regule al menos: controles de acceso, seguridad física y ambiental, identificación, manejo, custodia y responsabilidad sobre activos de información, procedimientos de respaldo y transferencia de información, protección contra malware, gestión de vulnerabilidades técnicas, seguridad en las comunicaciones, controles criptográficos	Etapa 1 de madurez. La institución no cuenta con una política de seguridad formalmente implantada, aprobada y socializada. Se han establecido esfuerzos puntuales respecto a la seguridad (roles, seguridad física de los servidores, protección contra malware, gestión de vulnerabilidades técnicas)	2	Medio
2	5.1.2 Revisiones a la política de seguridad	Evidencia de revisiones realizadas, conforme esté planificado en la política vigente. Cronograma de revisión para garantizar su actualización.	Etapa 1 de madurez. No se encuentra definida una política. Se procura actualizar medidas de seguridad conforme alertas recibida por parte del CSIRT de CEDIA.	2	Medio
A6. Organización de seguridad de la información					
3	6.1.1 Roles y responsabilidades de seguridad de la información	Identificación y definición de activos y procesos de seguridad Designación de responsables o procesos de seguridad Definición de niveles de autorización	Etapa 1 de madurez. No se encuentran identificados los activos y procesos de información. Existen custodios responsables de los activos hardware. Se encuentran definidos los niveles de autorización, pero no de forma documentada.	2	Medio

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
4	6.1.2 Separación de funciones	Privilegio de acceso, modificación o utilización de bases de datos, independiente del proceso de autorización. Excepción: evidencia de monitoreo, pistas de auditoría y supervisión.	Etapa 1 de madurez. Definidos roles y privilegios de DDL Y DML. Sin embargo no se realiza un monitoreo a las actividades del Administrador de Base de Datos.	2	Medio
5	6.1.3 Contacto con las autoridades	Definición de procesos de comunicación interno, con proveedores de servicios y autoridades en caso de incidentes de seguridad	Etapa 1 de madurez. Se notifica a la Dirección en caso de incidentes, se mantiene contacto con proveedores de servicio. No está definido un proceso	2	Medio
6	6.1.4 Contacto con grupos de interés especial	Miembro de grupos, foros o asociaciones profesionales especialidad en seguridad para manejo de mejores práctica, actualización, asesoramiento, tecnología, productos, amenazas y vulnerabilidades.	Etapa 2 de madurez. La institución forma parte de CEDIA quien por medio del equipo CSIRT alerta de forma permanente sobre nuevas amenazas y realiza un monitoreo al sistema de comunicaciones para informar sobre posibles vulnerabilidades.	3	Alto
7	6.1.5 Gestión de Proyecto de seguridad de la información	Proyecto de seguridad de la información	Etapa 1 de madurez. En coordinación para una posible ejecución de trabajos de titulación en el área de seguridad con los estudiantes de la carrera de Ingeniería en Sistemas. No ha sido considerado un proyecto de seguridad de la información dentro de la planificación institucional.	2	Medio

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
8	6.2.1 Política de dispositivo móvil	Política que contenga para equipos institucionales o personales: registro de dispositivos móviles, requisitos para la protección física, restricciones de instalación de software, versiones y parches, restricciones de conexión a servicios de información, controles de acceso, técnicas criptográficas, protección contra malware, inhabilitación, borrado y bloqueos remotos, copias de respaldo, utilización de servicios	Etapa 1 de madurez. Está permitido el acceso web a la aplicación del sistema académico para estudiantes y docentes. Acceso mediante credenciales. No se consideran restricciones.	2	Medio
9	6.2.2 Teletrabajo	Política de seguridad que considere: provisión de equipos, seguridad física, requisitos de seguridad en comunicaciones, sensibilidad de información a la que se accede, uso de equipos personales o de terceros, protección firewalls y contra malware.	Etapa 2 de madurez. Acceso mediante VPN únicamente con autorización del Coordinador	3	Alto
A7. Seguridad en recursos humanos					
10	7.1.1 Investigación de antecedentes	Cumplimiento de requisitos legales, competencias para el desempeño del cargo	Etapa 2 de madurez. Se cumplen los procedimientos de selección de personal establecidos por el Departamento de Administración del Talento Humano	3	Alto

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
11	7.1.2 Términos y condiciones laborales	Acuerdo de confidencialidad (acceso a información sensible) que contenga: responsabilidades respecto a la propiedad intelectual y protección de datos, acciones disciplinarias por incumplimiento	Etapa 2 de madurez. Implementado acuerdo de confidencialidad para operadores y usuarios de los sistemas	2	Medio
12	7.2.1 Responsabilidades de la Dirección	Elaboración y socialización de políticas de seguridad, directrices, plan de capacitación	Etapa 1 de madurez. Se encuentran asignadas las responsabilidades, pero no de forma documentada. No existe evidencia de un plan de capacitación institucional. Se realizan esfuerzos individuales para mantenerse actualizados.	2	Medio
13	7.2.2 Concienciación, educación y formación en seguridad de la información	Plan de concienciación respecto a conocimiento y aplicación de normas, responsabilidad de los usuarios, procedimientos básicos de seguridad	Inexistente. No se ha planificado ni ejecutado ningún programa de concienciación sobre seguridad de la información	1	Bajo
14	7.2.3 Proceso disciplinario	Implementación de procesos disciplinarios por violación de seguridad que considere naturaleza, gravedad, impacto, reincidencia.	Inexistente. No se cuenta con ninguna política o procedimiento al respecto	1	Bajo

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
15	7.3.1 Responsabilidad por finalización o cambio de empleo	Acuerdo de confidencialidad (acceso a información sensible) que contenga: responsabilidades por finalización o cambio laboral	Etapa 1 de madurez. Previo a la desvinculación laboral el funcionario debe validar el formulario de Paz y Salvo que entre sus requerimientos inhabilita credenciales de acceso y cierra cuentas de correo electrónico institucional. El cambio de área laboral no cuenta con un proceso definido de notificación para inhabilitación de credenciales o cambio de privilegios.	2	Medio
A.8 Gestión de activos					
16	8.1.1 Inventario de activos	Matriz de activos: primarios y de soporte	Inexistente. No se encuentran identificados los activos de información	1	Bajo
17	8.1.2 Propiedad de los activos	Custodio de activos. Activos inventariados, protegidos Definición de restricciones de acceso	Etapa 1 de madurez. No se cuenta con el inventario de activos Existen custodios responsables de los activos hardware. Se encuentran definidos los niveles de autorización, pero no de forma documentada.	2	Medio
18	8.1.3 Uso aceptable de los activos	Concienciación a usuarios y empleados sobre requisitos de seguridad para acceso a los activos de información	Etapa 1 de madurez. Se emiten indicaciones generales sobre cuidado de claves de acceso	2	Medio
19	8.1.4 Devolución de activos	Proceso de desvinculación que incluya documentación de conocimientos respecto a operaciones en curso, y la no autorización sobre el uso de información relevante	Etapa 1 de madurez. No se cuenta con un procedimiento formal sobre la confidencialidad de la información, y procesos de operación.	2	Medio
20	8.2.1 Clasificación de la información	Clasificación de la información de los	Inexistente. No se cuenta con el inventario de activos, y tampoco se	1	Bajo

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
		SGBD en función de la sensibilidad y criticidad	ha clasificado la información de los SGBD por su nivel de sensibilidad y criticidad		
21	8.2.2 Etiquetado de la información	Procedimiento definido para etiquetar y clasificar la información sensible	Inexistente. No se encuentra clasificada la información, por tanto no se cuenta con un procedimiento de etiquetado	1	Bajo
22	8.2.3 Manejo de activos	Procedimiento formal respecto a restricciones de acceso, manejo de copias de información, cumplimiento especificaciones del fabricante de los activos hardware	Etapa 2 de madurez. Se cumple el estándar TIER capa II para el Data Center. Respaldo diario automático de bases de datos, almacenamiento en medios extraíbles. No hay procedimiento formal definido	3	Alto
23	8.3.1 Gestión y transferencia de medios extraíbles	Procedimiento de registro, almacenamiento, criptografía, traslado, actualización, transferencia, borrado de información y desechar con seguridad medios que contengan información confidencial	Etapa 1 de madurez. Se ejecutan medidas básicas de seguridad	2	Medio
24	8.3.2 Eliminación de los medios	Procedimiento de borrado y eliminación segura de medios extraíbles que contengan información confidencial	Etapa 1 de madurez. Se ejecutan medidas básicas de seguridad	2	Medio
25	8.3.3 Transferencia de medios físicos	Procedimiento de transferencia de información por medios extraíbles que contengan información confidencial	Etapa 1 de madurez. Se ejecutan medidas básicas de seguridad	2	Medio
A.9 Control de acceso					
26	9.1.1 Política de control de acceso	Política de control de acceso a los activos de información que contenga: requisitos de seguridad, derechos de acceso en entornos interconectados,	Etapa 1 de madurez. Se han definido procedimientos para creación, inhabilitación y eliminación de usuario. No siempre son notificados los	2	Medio

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
		políticas de red, separación de funciones	requerimientos de revocación de derechos de acceso. Detectadas vulnerabilidades de riesgo medio a nivel de aplicación y local.		
27	9.1.2 Acceso a redes y servicios de red	Política de acceso a redes y servicios de red que contenga los procedimientos de autorización de privilegios, los medios de acceso, monitorización de uso	Etapa 1 de madurez. Separación de redes para estudiantes y docentes y servicios de acceso de red por tipo de usuario. Monitoreo de tráfico de red.	2	Medio
28	9.2.1 Registro y retiro de usuarios	Política de registro y retirada de usuarios que contenga responsabilidades y control de usuarios activos	Etapa 1 de madurez. La asignación de credenciales para el acceso a la red inalámbrica para los estudiantes es un proceso en línea interconectado con el sistema académico que otorga credenciales siempre y cuando cuente con una matrícula vigente. Valida historial de contraseñas y número máximo de caracteres. No admite caracteres especiales, sin embargo, no emite una alerta al respecto. El usuario no sabe que un carácter especial no fue admitido en su contraseña La asignación de credenciales para el personal docente es manual.	2	Medio
29	9.2.2 Provisión de accesos a usuarios	Política respecto a la asignación, modificación, revisión y revocación de accesos concedidos a usuarios.	Etapa 2 de madurez. El formulario Paz y Salvo permite revocar privilegios de acceso. No siempre son notificados los requerimientos de revocación de derechos de acceso, cuando hay	2	Medio

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
			cambios internos en la institución		
30	9.2.3 Gestión de privilegios de derechos de acceso	Política de asignación de derecho de acceso privilegiado a los SGBD conforme roles que incluya competencias y lista de usuarios	Etapa 2 de madurez. El personal que opera los sistemas y administra las bases de datos tienen privilegios específicos respecto al DDL y DML. Adecuada asignación de permisos por entidad.	3	Alto
31	9.2.4 Gestión de la información secreta de autenticación de los usuarios	Política de confidencialidad de datos de acceso por parte de los usuarios	Etapa 2 de madurez. El procedimiento de acceso al sistema académico por parte de estudiantes, docentes y operadores es mediante credenciales y privilegios conforme los roles de cada uno.	3	Alto
32	9.2.5 Revisión de los derechos de acceso de usuarios	Revisión periódica de derechos de acceso, para actualización o modificación de privilegios	Etapa 1 de madurez. Se cumple con el formulario Paz y Salvo y cuando es notificado por alguna dependencia. No se realiza una revisión periódica de derechos de acceso.	2	Medio
33	9.2.6 Retiro y ajuste de los derechos de acceso	Revisión periódica de derechos de acceso, para suspensión o eliminación de privilegios	Etapa 2 de madurez. Los privilegios de acceso son revocados con la legalización del formulario Paz y Salvo.	3	Alto
34	9.3.1 Uso de información secreta de autenticación	Capacitación a usuarios sobre confidencialidad de la información de autenticación	Etapa 1 de madurez. En los procesos de capacitación se imparten directrices generales sobre responsabilidad en el uso de contraseñas.	2	Medio
35	9.4.1 Restricción del acceso a la información	Privilegios de acceso por perfil de usuario Controles de acceso físico y lógico a las aplicaciones.	Etapa 3 de madurez. Se encuentran definidos los roles y privilegios de usuarios. La aplicación del sistema académico se instala únicamente en los equipos de los operadores autorizados. La activación de credenciales de acceso se realiza una vez	3	Alto

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
			cumplida la capacitación.		
36	9.4.2 Procedimientos seguros de inicio de sesión	Política de inicio seguro de sesión que permita una verificación robusta de la identidad del usuario utilizando métodos adicionales a las contraseñas.	Etapa 2 de madurez. Contraseñas con longitud mínima requerida, alfanuméricas. SHA-2. Codificación AES para la red inalámbrica.	3	Alto
37	9.4.3 Sistema de gestión de contraseñas	Implementación de un sistema de gestión de contraseñas interactivo con el usuario que contemple: selección de contraseñas de calidad, forzar cambio tras el primer inicio de sesión, almacenar archivos de contraseñas de manera separada de los datos del sistema de aplicación, transmisión protegida de las contraseñas	Etapa 2 de madurez. Sistema en línea para generación y recuperación de credenciales de acceso para acceder al sistema académico por parte de docentes y estudiantes. Algoritmo criptográfico SHA-2 Valida historial y longitud mínima. No admite caracteres especiales, pero no existe una alerta al usuario.	3	Alto
38	9.4.4 Uso de programas utilitarios privilegiados	Política de uso de programas utilitarios en servidores	Etapa 2 de madurez. No se encuentran instalados utilitarios en los servidores.	3	Alto
39	9.4.5 Control de acceso al código fuente del programa	Política de protección de código fuente	Etapa 3 de madurez. Acceso restringido conforme módulo desarrollado. Código fuente registrado en el IEPI	3	Alto
A.10 Criptografía					
40	10.1.1 Política de uso de los controles criptográficos	Política de uso de controles criptográficos	Etapa 1 de madurez. Protocolo AES para la WLAN. Credenciales de acceso con SHA-2	2	Medio
41	10.1.2 Gestión de llaves	Política que garantice la generación, almacenamiento, recuperación, distribución y destrucción de llaves	Etapa 1 de madurez. Protocolo AES para la WLAN. Credenciales de acceso con SHA-2	2	Medio
A.11 Seguridad física y del entorno					

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
42	11.1.1 Perímetro de seguridad física	Directrices de acceso a las instalaciones y área de los servidores, que incluya la seguridad física del entorno y los controles y usuarios autorizados para acceso.	Etapa 2 de madurez. Cumplimiento estándar TIER II. Restricciones de acceso solo para el personal del área de redes. Usuarios autorizados por medio de control biométrico y tarjeta de acceso.	3	Alto
43	11.1.2 Controles físicos de entrada	Procedimiento que verifique el acceso de usuarios mediante un control de acceso de visitantes, restricción a áreas controladas solo para personal autorizado	Etapa 2 de madurez. Cumplimiento estándar TIER II. Restricciones de acceso solo para el personal del área de redes. Usuarios autorizados por medio de control biométrico y tarjeta de acceso.	3	Alto
44	11.1.3 Seguridad de oficinas, despachos e instalaciones	Seguridad física de oficinas, e instalaciones, restricciones de acceso	Etapa 2 de madurez. Control de acceso de usuarios	3	Alto
45	11.1.1 Protección contra las amenazas externas y ambientales	Normas de seguridad para protección contra desastres naturales o intentos de ataque por personas	Etapa 2 de madurez. Diseño estructural antisísmico, estándares de seguridad eléctrica, contra incendios, etc. conforme especificaciones de organismos de control competentes. Servicio de seguridad privada.	3	Alto
46	11.1.5 Trabajo en áreas seguras	Protocolos de trabajo seguro para el personal	Etapa 1 de madurez. En operación el equipo multidisciplinario para evaluación de emergencias y desastres	2	Medio
47	11.1.6 Áreas de carga y entrega	Procedimientos seguros para recepción de equipos en el área de servidores, que incluya: prevención de ingreso de materiales que puedan comprometer o interferir las comunicaciones	Etapa 2 de madurez. Procedimiento de validación de credenciales. Registro de equipos y materiales que ingresan y salen. Control de equipos que causen interferencia.	3	Alto
48	11.2.1 Ubicación y protección de equipos	Directrices de ubicación de equipos que garantice la seguridad física,	Etapa 2 de madurez. Cumplimiento estándar TIER II.	3	Alto

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
		ambiental y de comunicaciones			
49	11.2.2 Instalaciones de suministro	Protección de los equipos contra fallos de alimentación. Cumplimiento de normativas respecto a seguridad de las instalaciones eléctricas y de telecomunicaciones	Etapa 2 de madurez. Cumplimiento estándar TIER II.	3	Alto
50	11.2.3 Seguridad del cableado	Políticas de protección de cableado eléctrico y de telecomunicaciones para protección contra interceptaciones, interferencias o daños que contemple al menos: soterramiento o medidas alternativas de protección, separación de cables de energía y de comunicaciones, conductos blindados, control de acceso a paneles de parcheo	Etapa 2 de madurez. Cumplimiento estándar TIER II.	3	Alto
51	11.2.4 Mantenimiento de los equipos	Plan de mantenimiento preventivo y correctivo	Etapa 2 de madurez. Plan anual de mantenimiento de redes e infraestructura.	3	Alto
52	11.2.5 Eliminación de activos	Formulario de registro de entrada y salida de activos: equipos, software, información.	Inexistente. No se tiene control sobre salida de activos de información.	1	Bajo
53	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	Directrices de seguridad en caso de requerirse la salida de un equipo que almacene o trate información institucional	Etapa 1 de madurez. Los equipos cuentan con custodios, pero no hay definidas políticas de protección, solo se considera la responsabilidad del custodio sobre el equipo.	2	Medio
54	11.2.7 Reutilización o eliminación segura de equipos	Directriz respecto a la reutilización de equipos previa confirmación de no contener información sensible o software bajo licencia que no haya sido	Etapa 2 de madurez. Informe técnico respecto a la funcionalidad del equipo. Formateo de equipo previa entrega a nuevo custodio.	3	Alto

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
		eliminado de manera segura			
55	11.2.8. Equipos de usuario desatendido	Capacitación a usuarios sobre necesidad de cierre de sesiones cuando ya no se va a operar los sistemas	Etapa 1 de madurez. Se generan directrices generales en los procesos de capacitación	2	Medio
56	11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Capacitación a usuarios sobre custodia y almacenamiento adecuado de información sensible	Etapa 2 de madurez. Equipos de operadores cuentan con credenciales de acceso.	3	Alto
A.12 Seguridad de las operaciones					
57	12.1.1 Documentación de procedimientos de operación	Documentación de procedimientos de operación de los sistemas	Etapa 1 de madurez. Manuales técnico y de usuario	2	Medio
58	12.1.2 Gestión de cambios	Directrices para controlar cambios significativos en los sistemas, evaluando su impacto y afectación a la disponibilidad	Etapa 2 de madurez. Se realizan pruebas funcionales previa actualización	2	Medio
59	12.1.3 Gestión de capacidades	Plan de gestión de capacidad de los sistemas, recursos humanos e instalaciones.	Etapa 1 de madurez. Decisiones conforme mantenimiento realizado. Evaluación sobre demanda. No se cuenta con un plan de gestión	2	Medio
60	12.1.4 Separación de ambientes de desarrollo, pruebas y producción	Definición de reglas para la operación, transferencia de software, cambio de aplicaciones y perfiles de usuario para los ambientes de desarrollo, prueba y producción	Etapa 2 de madurez. Manejo de ambientes separados para desarrollo pruebas y producción. Credenciales de acceso diferentes para cada sistema	3	Alto
61	12.2.1 Controles contra malware	Políticas sobre la prohibición de uso de software no autorizado, listas negras, reducción de vulnerabilidades, responsabilidades de gestión de protección de sistemas	Etapa 2 de madurez. Congelamiento de equipos. Bloqueo de puertos. Gestión de vulnerabilidades técnicas a través del CSIRT de CEDIA.	3	Alto

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
62	12.3.1 Copias de seguridad de la información	Políticas de copias de seguridad	Etapa 1 de madurez. Respaldo diario automático de bases de datos, almacenamiento en medios extraíbles. Reposan en la misma área	2	Medio
63	12.4.1 Registro de eventos	Plan de registro, protección y revisión periódica de las actividades de los usuarios, excepción, fallos y eventos de seguridad de la información	Etapa 1 de madurez. Definidos niveles de seguridad y privilegios de acceso.	2	Medio
64	12.4.2 Protección de la información de registro	Controles contra cambios no autorizados	Etapa 1 de madurez. Definidos niveles de seguridad y privilegios de acceso.	2	Medio
65	12.4.3 Registros de administración y operación	Supervisión de las actividades ejecutadas por los administradores de base de datos.	Etapa 1 de madurez. Definidos niveles de seguridad y privilegios de acceso.	2	Medio
66	12.4.4 Sincronización del reloj	Sincronización de relojes con una única fuente acordada de tiempo	Etapa 2 de madurez. Sincronización UTC	3	Alto
67	12.5.1 Instalación del software en los sistemas operativos	Directrices de control de instalación de software en sistemas en producción	Etapa 2 de madurez. Pruebas de usabilidad. Registro de versiones anteriores.	3	Alto
68	12.6.1 Gestión de las vulnerabilidades técnicas	Inventario de activos, control de actualización, identificación de vulnerabilidades técnicas por desactualización de software, análisis de riesgos asociados	Etapa 1 de madurez. Se actualizan los sistemas operativos	2	Medio
69	12.6.2 Restricciones en la instalación del software	Política de restricción de instalación de software	Etapa 2 de madurez. Congelamiento de equipos.	3	Alto
70	12.7.1 Controles de auditoría de sistemas de información	Planificación de controles de auditoría	Etapa 2 de madurez. Implementado un registro de auditoría de transacciones	3	Alto
A.13 Seguridad en las comunicaciones					
71	13.1.1 Controles de red	Administración de la red, permisos, registro de eventos y monitorización	Etapa 2 de madurez. Administración de red. Monitoreo de vulnerabilidades con	3	Alto

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
			colaboración del CSIRT de CEDIA. Acceso autenticado a los servicios de red.		
72	13.1.2 Seguridad de los servicios de red	Tecnología, autenticación, conexión segura, acceso por aplicaciones	Etapa 2 de madurez. Protocolo AES para la WLAN. Vlans, dominios de red. Restricción por puerto, no por aplicaciones.	3	Alto
73	13.1.3 Separación en las redes	Gestión de dominios de red, seguridades, interconexiones externas	Etapa 2 de madurez. Protocolo AES para la WLAN. Vlans, dominios de red. Restricción por puerto, no por aplicaciones.	3	Alto
74	13.2.1 Políticas y procedimientos de transferencia de información	Protocolos de seguridad para la transferencia de información en la red	Etapa 1 de madurez. No se cuenta con el inventario de activos. No está clasificada la información por su nivel de sensibilidad y criticidad.	2	Medio
75	13.2.2 Acuerdos de transferencia de información	Acuerdos de transferencia de información que contenga responsabilidades y procedimientos	Etapa 1 de madurez. Protocolo AES para la WLAN. SHA-2 para credenciales del sistema.	3	Alto
76	13.2.3 Mensajería electrónica	Procedimientos de seguridad. Tipo de accesos permitidos	Inexistente. No se cuenta con una política que regule la transferencia de información por mensajería electrónica (correo electrónico, redes sociales, etc.)	1	Bajo
77	13.2.4 Acuerdos de confidencialidad o no revelación	Acuerdos de confidencialidad	Etapa 1 de madurez. En fase de implementación acuerdo de confidencialidad con operadores y usuarios.	2	Medio
A.14 Adquisición, desarrollo y mantenimiento del sistema					
78	14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Requisitos de seguridad en la planificación de nuevos proyectos	Etapa 2 de madurez. Planificado niveles y privilegios de acceso. Auditoría de transacciones. Pruebas de funcionalidad	3	Alto
79	14.1.2 Asegurar los servicios de aplicaciones en redes públicas	Protocolos de seguridad para los servicios de aplicaciones que se	Etapa 2 de madurez. Credenciales con SHA-2. Codificación AES para la red inalámbrica.	3	Alto

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
		transmiten a través de redes públicas	Certificado digital para la plataforma Uvirtual		
80	14.1.3 Protección de las transacciones de servicios de aplicaciones	Certificados digitales para información sensible	Etapa 2 de madurez. Credenciales con SHA-2. Codificación AES para la red inalámbrica. Certificado digital para la plataforma Uvirtual	3	Alto
81	14.2.1 Política de desarrollo seguro	Procedimientos de seguridad en el ciclo de vida de desarrollo de sistemas de información	Etapa 2 de madurez. Planificados controles de seguridad para las aplicaciones y las bases de datos. Niveles de privilegio de acceso. Pruebas de funcionalidad	3	Alto
82	14.2.2 Procedimientos de control de cambios en sistemas	Políticas de control de cambios, análisis de riesgos, pruebas	Etapa 2 de madurez. Considerados en la planificación control de cambios, análisis de riesgos y pruebas, control de versiones. Manejo separado de ambientes de producción, pruebas y desarrollo	3	Alto
83	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Procedimientos formales de control de cambios a lo largo del ciclo de vida del software	Etapa 2 de madurez. Considerados en la planificación control de cambios, análisis de riesgos y pruebas, control de versiones. Manejo separado de ambientes de producción, pruebas y desarrollo	3	Alto
84	14.2.4 Restricciones a los cambios en los paquetes de software	Políticas de control de cambios, análisis de riesgos, pruebas	Etapa 2 de madurez. Considerados en la planificación control de cambios, análisis de riesgos y pruebas, control de versiones. Manejo separado de ambientes de producción, pruebas y desarrollo	3	Alto
85	14.2.5 Principios de ingeniería de sistemas seguros	Principios de ingeniería de sistemas seguros.	Etapa 2 de madurez. Considerados en la planificación control de cambios, análisis de riesgos y pruebas, control de versiones. Manejo separado de	3	Alto

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
			ambientes de producción, pruebas y desarrollo		
86	14.2.6 Ambiente de desarrollo seguro	Política de desarrollo seguro que contemple las personas, los procesos y la tecnología	Etapa 2 de madurez. Considerados en la planificación control de cambios, análisis de riesgos y pruebas, control de versiones. Manejo separado de ambientes de producción, pruebas y desarrollo	3	Alto
87	14.2.7 Desarrollo externalizado	Procedimiento de seguridad respecto a licencias, propiedad del código, seguridades, pruebas	Etapa 1 de madurez. Procedimientos conforme términos de referencia establecidos	2	Medio
88	14.2.8 Pruebas de seguridad del sistema	Directrices de pruebas de seguridad	Etapa 2 de madurez. Considerados en la planificación control de cambios, análisis de riesgos y pruebas, control de versiones. Manejo separado de ambientes de producción, pruebas y desarrollo	3	Alto
89	14.2.9 Pruebas de aceptación de sistemas	Directrices para pruebas de aceptación	Etapa 2 de madurez. Considerados en la planificación control de cambios, análisis de riesgos y pruebas, control de versiones. Manejo separado de ambientes de producción, pruebas y desarrollo	3	Alto
90	14.3.1 Protección de los datos de prueba	Política de utilización de datos de prueba	Etapa 2 de madurez. Plan de pruebas	3	Alto
A.15 Relaciones con proveedores					
91	15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Política de acceso a la información en relaciones con proveedores	Etapa 1 de madurez. Cumplimiento de Ley de Contratación Pública. Regulaciones con proveedores conforme términos de referencia establecidos	2	Medio

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
92	15.1.2 Requisitos de seguridad en contratos con terceros	Política de términos contractuales	Etapa 1 de madurez. Cumplimiento de Ley de Contratación Pública. Regulaciones con proveedores conforme términos de referencia establecidos	2	Medio
93	15.1.3 Cadena de suministro de tecnologías de la información y de las comunicaciones	Requisitos de seguridad para la cadena suministro	Etapa 1 de madurez. Cumplimiento de Ley de Contratación Pública. Regulaciones con proveedores conforme términos de referencia establecidos	2	Medio
94	15.2.1 Monitoreo y revisión de los servicios de proveedores	Política de monitoreo de los servicios de los proveedores respecto a la seguridad de la información	Etapa 1 de madurez. Cumplimiento de Ley de Contratación Pública. Regulaciones con proveedores conforme términos de referencia establecidos	2	Medio
95	15.2.2 Gestión de cambios en los servicios de proveedores	Política de control y supervisión de cambios de servicios recibidos por terceros.	Etapa 1 de madurez. Cumplimiento de Ley de Contratación Pública. Regulaciones con proveedores conforme términos de referencia establecidos	2	Medio
A.16 Gestión de incidentes de seguridad de la información					
96	16.1.1 Responsabilidades y procedimientos	Responsabilidades y procedimientos para detectar, registrar, manejar y evaluar y actuar frente a eventos de seguridad	Etapa 1 de madurez. No se encuentra definida una política. Se procura actualizar medidas de seguridad conforme alertas recibida por parte del CSIRT de CEDIA.	2	Medio
97	16.1.2 Informe de los eventos de seguridad de la información	Política de comunicación respecto a eventos de seguridad	Etapa 1 de madurez. Se notifica al Director de la Unidad en caso de eventos de seguridad	2	Medio
98	16.1.3 Informe de debilidades de seguridad de la información	Concienciación a usuarios sobre la necesidad de notificar posibles vulnerabilidades detectadas en los sistemas de información	Inexistente. No se han realizado procesos de capacitación a usuarios	1	Bajo

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
99	16.1.4 Apreciación y decisión sobre los eventos de seguridad de la información	Directriz para evaluación de eventos de seguridad y acciones de solución	Etapa 1 de madurez. Se ejecutan procedimientos de seguridad puntuales conforme se produzcan eventos de seguridad	2	Medio
100	16.1.5 Respuesta a incidentes de seguridad de la información	Acciones y documentación respecto a incidentes de seguridad	Etapa 1 de madurez. Notificación de incidentes. Tratamiento de la vulnerabilidad	2	Medio
101	16.1.6 Aprendizaje de los incidentes de seguridad de la información	Monitoreo y evaluación de incidentes de seguridad para analizar requerimientos de seguridad	Etapa 1 de madurez. Tratamiento de la vulnerabilidad	2	Medio
102	16.1.7 Recopilación de evidencias	Documentación respecto a los incidentes de seguridad	Etapa 1 de madurez. Notificación de incidentes. Tratamiento de la vulnerabilidad	2	Medio
A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio					
103	17.1.1 Planificación de la continuidad de seguridad de la información 17.1.2 Implementación de la continuidad de seguridad de la información 17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información	Política de seguridad de la información en situaciones adversas o desastres, su implementación, revisión periódica y evaluación	Etapa 2 de madurez. Designación de responsables para mitigación de eventos de seguridad	3	Alto
104	17.2.1 Disponibilidad de las instalaciones de procesamiento de la información	Directrices de redundancia de los sistemas	Etapa 2 de madurez. Estándar TIER II	3	Alto
A.18 Cumplimiento					
105	18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Leyes, reglamentos y normativas vigentes respecto al negocio de la institución	Etapa 3 de madurez. Identificada y aplicada la normativa legal interna y externa que rige el funcionamiento de la institución	3	Alto

No	Control	Resultado esperado	Resultado Obtenido (estado actual)	Nivel de Madurez	
				Valoración	Equivalencia
106	18.1.2 Derechos de propiedad intelectual	Política de propiedad intelectual respecto a los activos de información	Etapa 3 de madurez. Código fuente registrado en el IEPI. Licencias de software de programas propietarios. Protección de derechos de autor	3	Alto
107	18.1.3 Protección de los registros	Identificación, clasificación, conservación y manejo de los registros de información	Inexistente. No se tienen identificados los registros de información	1	Bajo
108	18.1.4 Protección y privacidad de la información de carácter personal	Política de protección de datos personales	Etapa 1 de madurez. En fase de implementación acuerdo de confidencialidad con operadores y usuarios.	2	Medio
109	18.1.5 Reglamentos de controles criptográficos	Política de uso de controles criptográficos	Etapa 2 de madurez. Contraseñas con longitud mínima requerida, alfanuméricas. SHA-2. Codificación AES para la red inalámbrica. Certificado digital para la plataforma Uvirtual	3	Alto
110	18.2.1 Revisión independiente de seguridad de la información	Directriz de revisión independiente, por parte del nivel directivo, de las políticas de seguridad de la información para garantizar su efectividad	Inexistente. No se realizan controles independientes por parte de la Dirección	1	Bajo
111	18.2.2 Cumplimiento de las políticas y normas de seguridad	Monitoreo, evaluación y acciones correctivas al cumplimiento de políticas de seguridad	Inexistente. No existe un monitoreo o evaluación de cumplimiento de políticas de seguridad	1	Bajo
112	18.2.3 Comprobación del cumplimiento técnico	Planificación y evaluación del cumplimiento técnico de los sistemas para analizar vulnerabilidades	Etapa 1 de madurez. No se encuentra definida una política. Se procura actualizar medidas de seguridad conforme alertas recibida por parte del CSIRT de CEDIA.	2	Medio

Fuente: Matriz de evaluación nivel de madurez controles de seguridad
Elaborado por: La Investigadora

ENCUESTAS

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
MAESTRÍA EN GESTIÓN DE BASE DE DATOS – III VERSIÓN

Encuesta dirigida al personal Directivo, Administradores de las Bases de Datos y personal técnico del Centro de Tecnología Educativa, para determinar el nivel de manejo de políticas de seguridad de la información respecto a los SGBD.
(Aplicación de preguntas con base a las especificaciones de las normas ISO 27001 y 27002)

Lea las preguntas y considere la siguiente escala que le permita valorar el nivel de cumplimiento de cada uno de los aspectos mencionados. Desarrolle su respuesta cuando sea requerida.

Puntuación	Valor	Referencia conceptual
0	Nulo	No existe información documentada o no se ha implementado el control.
1	Bajo	Se han implementado esfuerzos puntuales respecto a la seguridad, pero no de forma documentada o sistemática.
2	Medio	Se cuenta con evidencia documental que permite establecer un mayor esfuerzo por la gestión de los riesgos de seguridad, al menos en aspectos básicos.
3	Alto	Está implementado un control documentado respecto a la seguridad de la información, su monitoreo y tratamiento.

1. A.5 Política de seguridad de la información

No	Pregunta	Puntuación
1	¿Está implementada, aprobada, socializada y disponible para su acceso una política de seguridad de la información para los SGBD en la institución?.	
2	¿La política de seguridad prevé realizar revisiones de actualización?	

2. A.6 Organización de seguridad de la información

No	Pregunta	Puntuación
3	¿Se encuentran identificadas y definidas las responsabilidades y procesos de seguridad de la información?	
4	¿Se encuentran definidos los roles y privilegios para acceso y manipulación de la información de los SGBD?	

5	¿Se monitorea y supervisa la actividad de los usuarios y administradores de bases de datos?	
6	¿Se encuentra definido un procedimiento de comunicación con el nivel jerárquico superior cuando se requiere reportar incidentes de seguridad?	
7	¿Es parte la institución de algún grupo de interés especial que permita mantener actualizada información respecto amenazas y vulnerabilidades?	
8	¿Se cuenta con algún proyecto de seguridad de la información?	
9	¿Se han implementado controles de seguridad para el acceso a los SGBD desde dispositivos móviles?	
10	¿Se han implementado controles de seguridad para el acceso a los SGBD desde lugares remotos?	

3. A.7. Seguridad en recursos humanos

No	Pregunta	Puntuación
11	¿El personal que maneja los SGBD tiene las competencias necesarias para el cargo?	
12	¿Se ha implementado en la relación contractual con los empleados que manejan los SGBD algún acuerdo de confidencialidad y protección de datos?	
13	De ser afirmativa su respuesta. ¿El acuerdo considera las responsabilidades en la finalización de su relación laboral?	
14	¿El directivo de la unidad se preocupa de elaborar y socializar políticas o directrices de seguridad, así como un plan de capacitación para el personal?	
15	¿Se cuenta con algún programa de concienciación a los usuarios sobre seguridad de la información?	
16	¿Se ha implementado algún proceso disciplinario que garantice la seguridad de la información por parte de los usuarios?	

4. A.8 Gestión de activos

No	Pregunta	Puntuación
17	¿Se cuenta con el inventario de los activos de información?	
18	¿Los activos cuentan con un custodio?	

19	¿Se han emitido directrices para usuarios y empleados sobre requisitos de seguridad para acceso a los activos de información?	
20	¿Existe una política de desvinculación que incluya dejar documentado el conocimiento respecto a operaciones en curso y la no autorización sobre el uso de información relevante?	
21	¿Existe un inventario de la información contenida en los SGBD, y clasificada por su sensibilidad y criticidad?	
22	¿Cuentan la institución con procedimiento definido para etiquetar y clasificar la información sensible?	
23	¿Cuenta la institución con un procedimiento formal respecto al manejo de copias de seguridad y cumplimiento de especificaciones del fabricante respecto a los activos hardware?	
24	¿Existe alguna política para el tratamiento de medios extraíbles que contengan información de los SGBD, respecto a su registro, almacenamiento, traslado, criptografía, actualización, transferencia y borrado de información?	
25	¿Existe algún procedimiento para almacenar y desechar con seguridad medios que contengan información confidencial?	

5. A.9 Control de acceso

No	Pregunta	Puntuación
26	¿Existe alguna política referente al control de acceso, basada en los requisitos de negocio y de seguridad de la información?	
27	¿Se encuentra definido los roles y tipo de acceso por medio de los cuales los usuarios pueden acceder a través de redes a la información de los SGBD?	
28	¿Existe un procedimiento formal de registro y retirada de usuarios para asignación de derechos de acceso?	
29	¿Existe un procedimiento formal para asignar o revocar derechos de acceso a los SBGD?	
30	¿El acceso a información sensible ¿maneja algún procedimiento de control de acceso, autenticación y manipulación?	
31	¿Existe alguna planificación de revisión periódica de derechos de acceso de los usuarios?	
32	¿Se ha capacitado a los usuarios sobre prácticas de seguridad de la información?.	

33	¿Están implementadas políticas de control de acceso a la información, de acuerdo a las funciones y aplicaciones del sistema?	
34	¿Se cuenta con procedimientos seguros de inicio de sesión para el acceso a los sistemas y las aplicaciones?	
35	¿Se ha implementado un sistema de gestión de contraseñas?	
36	¿Se cuenta con alguna política respecto a la utilización de programas utilitarios en los SGBD?	
37	¿Existe alguna política respecto al acceso al código fuente de los programas?	

6. A.10 Criptografía

No	Pregunta	Puntuación
38	¿Se usa algún control criptográfico para proteger la confidencialidad, autenticidad e integridad de la información?	
39	De ser afirmativa su respuesta: ¿Existe alguna política que regule el uso y duración de las llaves criptográficas?.	

7. A.11 Seguridad física y del entorno

No	Pregunta	Puntuación
40	¿Se cuenta con alguna directriz de acceso y seguridad de las instalaciones y área de los servidores donde se maneja los servidores de SGBD?	
41	¿Se cuenta con alguna restricción de entrada y acceso únicamente para personal autorizado?	
42	¿Se cuenta con algún tipo de seguridad física de acceso al área de los servidores donde se encuentran los SGBD?	
43	¿Se cuenta con protección física contra desastres naturales, ataques intencionados o accidentes que puedan comprometer la información almacenada en los SGBD?	
44	¿En el área de servidores donde se encuentra los SGBD se maneja procedimientos de trabajo seguro para el personal responsable?	
45	¿Existe alguna política respecto a la ubicación de los equipos en lugares que garanticen la seguridad física, ambiental y de comunicaciones?	

46	¿Cuentan los equipos con sistemas de protección contra fallas en el sistema de alimentación eléctrica que pueda provocar daños a los mismos?	
47	¿Los sistemas de cableado eléctrico y de telecomunicaciones que transmite datos o da soporte a los servicios, cuentan con protección contra daños, interferencias o interceptaciones de información?	
48	¿Se cuenta con algún plan periódico de mantenimiento de equipos que garantice la disponibilidad e integridad de información?	
49	¿Se cuenta con algún control para autorización de salida de activos de la institución?	
50	¿Se cuenta con algún control que permita garantizar la reutilización de equipos, previa confirmación de no mantener información sensible o software bajo licencia que haya sido eliminado de manera segura, previa reutilización?	
51	¿Se ha capacitado a los usuarios sobre la importancia de realizar los cierres de sesión cuando ya no se va a operar los sistemas?	
52	¿Se cuenta con alguna política de puesto de trabajo despejado de papeles y medios de almacenamiento extraíbles? Para evitar acceso a información sensible?.	

8. A.12 Seguridad de las operaciones

53	¿Se cuenta con documentación de los procedimientos de operación de los SGBD, y estos están disponibles para los usuarios que lo necesitan?	
54	¿Se cuenta con un plan que permita prever los requisitos futuros de capacidad del sistema, para asegurar su desempeño adecuado?	
55	¿Se maneja por separado los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción?.	
56	¿Se cuenta con controles de detección, prevención y recuperación para protección contra un malware, así como procedimientos de concienciación al usuario?	
57	¿Se ha implementado alguna política de copias de seguridad?	
58	¿Se registra, protege y revisa periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información?	

59	¿Se registra, protege y revisa periódicamente las actividades de los administradores y del operador del sistema?	
60	¿Los relojes de los sistemas de procesamiento de información están sincronizados con una única fuente precisa y acordada de tiempo?	
61	¿Se cuenta con alguna política que regule la instalación de software en los sistemas operativos?.	
62	¿Se han realizado pruebas de la vulnerabilidad técnica de los sistemas de información utilizados?	
63	¿Se han realizado auditorías para la comprobación a los sistemas de información, considerando la interrupción mínima de los procesos de negocio?	

9. A.13 Seguridad en las comunicaciones

No	Pregunta	Puntuación
64	¿Se cuenta con algún control para la gestión de redes que permita proteger la información en los sistemas y aplicaciones?	
65	¿Se han establecido los mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red; tanto los que provee la institución, como los que se contrata?.	
66	¿Se maneja por separado en las redes los servicios de información, usuarios y sistemas de información.	
67	¿Se cuenta con alguna política que establezca el procedimiento de transferencia de información por cualquier recurso de comunicación?	
68	De ser afirmativa su respuesta ¿Se cuenta con acuerdos para la transferencia segura de información del negocio y software entre la organización y terceros?.	
69	¿Se cuenta con alguna política para la recepción, envío y manipulación de información a través de mensajería electrónica?	
70	¿Se ha implementado alguna política respecto a los acuerdos de confidencialidad o de no divulgación para la protección de la información?	

10. A.14 Adquisición, desarrollo y mantenimiento del sistema

No	Pregunta	Puntuación
71	¿Se consideró los requisitos relacionados con la seguridad de la información en los requisitos cuando se desarrolla, adquiere o mejora los sistemas de información existentes?.	

72	¿Se cuenta con controles de seguridad para la información que pasa a través de redes públicas contra fraude, disputa de contrato, revelación y modificación no autorizados?.	
74	¿Se ha implementado controles que garanticen que la información involucrada en transacciones de servicios de aplicaciones esté protegida para prevenir transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensajes no autorizados?.	
75	¿Se consideran políticas de desarrollo seguro de software en la institución?.	
76	¿Se cuenta con procedimientos formales de control de cambios a lo largo del ciclo de vida del software?	
77	¿Se cuenta con procedimientos que garanticen la disponibilidad de la información cuando se requiere modificaciones de sistemas operativos, para evitar efectos adversos en las operaciones o la seguridad de la información?-	
78	¿Se ha implementado alguna política para la restricción a los cambios a los paquetes de software, que limite los mismos a los estrictamente necesarios y que sean objeto de un control riguroso?	
79	¿Se han implementado, documentado y mantenido principios de ingeniería de sistemas seguros para los sistemas de información?	
80	¿Se considera alguna política que garantice ambientes de desarrollo seguro para el desarrollo de sistemas y que los esfuerzos de integración cubran todo el ciclo de vida de desarrollo del sistema?	
81	¿Se cuenta con una política que permita supervisar y controlar el desarrollo de software externalizado?	
82	¿Se cuenta con una política que establezca la necesidad de realizar pruebas de seguridad funcional durante el desarrollo?	
83	¿Se cuenta con una política que establezca la necesidad de contar con programas de pruebas de aceptación y criterios para nuevos sistemas de información, actualizaciones y nuevas versiones?.	
84	¿Se cuenta con una política que permita determinar el tipo y datos a ser utilizados para prueba, su protección y control?.	

11. A.15 Relación con proveedores

No	Pregunta	Puntuación
85	¿Se cuenta con una política que establezca los mecanismos de seguridad asociados con el acceso del proveedor y/o terceros a los activos de la organización?.	
86	¿Se cuenta con una política que establezca los requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos?.	
87	¿Se cuenta con alguna política que permita monitorear, revisar y auditar regularmente la provisión de servicios de los proveedores?.	
88	¿Se cuenta con alguna política que permita gestionar los cambios en la provisión de servicios, incluyendo mantenimiento y mejora de políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados, así como la reapreciación de los riesgos?.	

12. A.16 Gestión de incidentes de seguridad de la información

No	Pregunta	Puntuación
89	¿Se cuenta con una política que establezca las responsabilidades y procedimientos de gestión que aseguren una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información?	
90	¿Se cuenta con una política que establezca cómo deben ser notificados los incidentes de seguridad de la información?	
91	¿Se cuenta con una política que garantice que todos empleados y contratistas que utilizan los sistemas y servicios de información de la organización deben informar sobre cualquier debilidad de seguridad que observen o sospechen que exista en los sistemas o servicios?	
92	¿Se cuenta con una política que permita clasificar los eventos de seguridad, para determinar si se consideran incidentes?	
93	¿Se cuenta con alguna política que determine como deben ser atendidos los incidentes de seguridad y su documentación?	
94	¿Se cuenta con una política que permita identificar, recolectar y conservar información que pueda servir como evidencia respecto a los incidentes de seguridad?	

13. A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio

No	Pregunta	Puntuación
95	¿Se cuenta con una política que garantice la continuidad de la seguridad de la información en situaciones adversar por ejemplo, durante una crisis o desastre?	
96	¿Se planifica la revisión regular de los controles de continuidad de seguridad de la información, para asegurar que son válidos y eficaces durante situaciones adversas?.	
97	¿Se cuenta con una política de redundancia de la información que garanticen la disponibilidad de la misma?	

14. A.18 Cumplimiento

No	Pregunta	Puntuación
98	¿Se cuenta con una legislación que garantice el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados a la seguridad de la información de cada sistema de información de la institución?.	
99	¿Se cuenta con regulación para el uso de material sobre el cual pueda existir derechos de propiedad intelectual y sobre el uso de productos de software patentado?.	
100	¿Se cuenta con una regulación que proteja contra la pérdida, destrucción, falsificación, revelación o acceso no autorizado a los registros de información?	
101	¿Se cuenta con una regulación para la protección y privacidad de la información de carácter personal?.	
102	¿Se cuenta con una regulación para el manejo de controles criptográficos?	
103	¿Se cuenta con una planificación que permita revisar de forma periódica los controles de seguridad de la información?	
104	¿Se cuenta con una planificación que permita revisar de forma periódica el cumplimiento de las políticas, regulaciones o normas respecto a la seguridad de la información?	
105	¿Se cuenta con una planificación que permita revisar de forma periódica que los sistemas de información cumplen con las políticas y normas de seguridad de la información implementadas?	

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
MAESTRÍA EN GESTIÓN DE BASE DE DATOS – III VERSIÓN

Encuesta dirigida a los operadores de sistemas de Gestión de Base de Datos para determinar el nivel de manejo de políticas de seguridad de la información respecto a los SGBD.
(Aplicación de preguntas con base a las especificaciones de las normas ISO 27001, 27002 y 27005)

Lea las siguientes preguntas: Marque su respuesta con una X para los casos que corresponda y desarrolle su respuesta de forma completa, cuando sea requerida.

No	Pregunta	Opciones de respuesta
Política de seguridad de la información		
1	¿Conoce usted si la institución ha implementado alguna política de seguridad de la información para los sistemas a los que accede?	Si: ☐ No: ☐
Seguridad en recursos humanos		
2	¿Ha recibido capacitación para el manejo de sistemas?	Si: ☐ No: ☐
3	¿Existe alguna política respecto al acceso y divulgación de información contenida en los sistemas que usted opera?	Si: ☐ No: ☐
4	¿Ha sido sancionado alguna vez por proporcionar información sin autorización de los sistemas a los que tiene acceso?	Si: ☐ No: ☐
5	¿Ha sido llamado la atención o sancionado alguna vez por manejo inadecuado de claves de usuario?	Si: ☐ No: ☐
6	Si usted ha cambiado de función o salido de alguna otra área de trabajo en la institución. ¿Sabe si su usuario y privilegios de acceso anteriores fueron inhabilitados?	Si: ☐ No: ☐
7	De mantener aún acceso a sistemas de alguna función anterior. ¿Ha ingresado usted a dichos sistemas?	Si: ☐ No: ☐

Gestión de activos		
8	¿Conoce usted si alguna información de la que usted accede tiene restricción de divulgación?	Si: ☐ No: ☐
Control de acceso		
9	¿Ha recibido alguna capacitación sobre prácticas de seguridad de la información?	Si: ☐ No: ☐
10	Ha experimentado dificultades de acceso al sistema	Nunca: ☐ Alguna vez: ☐ A menudo: ☐
11	Las dificultades se han ocasionado por:	a Ingreso equivocado u olvido de claves de acceso ☐ b Sistema no disponible ☐ c Demora en la conexión ☐
12	¿Ha socializado sus datos de usuario de acceso con alguna otra persona?	Si: ☐ No: ☐

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
MAESTRÍA EN GESTIÓN DE BASE DE DATOS – III VERSIÓN

Encuesta dirigida a los usuarios de los sistemas de Gestión de Base de Datos para determinar el nivel de manejo de políticas de seguridad de la información respecto a los SGBD.
(Aplicación de preguntas con base a las especificaciones de las normas ISO 27001 y 27002)

Lea las siguientes preguntas: Marque su respuesta con una X para los casos que corresponda y desarrolle su respuesta de forma completa, cuando sea requerida.

No	Pregunta	Opciones de respuesta
Política de seguridad de la información		
1	¿A qué sistema académico institucional tiene acceso?	SICOA estudiantes: ☐ SICOA Docentes: ☐
2	¿Conoce usted si la institución ha implementado alguna política de seguridad de la información para los sistemas a los que accede?	Si: ☐ No: ☐
Organización de seguridad de la información		
3	¿Se encuentra su equipo de cómputo protegido y actualizado contra malware?	Si: ☐ No: ☐
Seguridad en recursos humanos		
4	¿Ha recibido capacitación para el manejo del sistema?	Si: ☐ No: ☐
Gestión de activos		
5	¿Conoce usted si la institución tiene alguna política de protección de datos y divulgación de información?	Si: ☐ No: ☐
6	¿Conoce usted si alguna información de la que usted accede tiene restricción de divulgación?	Si: ☐ No: ☐
Control de acceso		
7	¿Ha recibido alguna capacitación institucional sobre prácticas de seguridad de la información?	Si: ☐ No: ☐

8	Ha experimentado dificultades de acceso al sistema	Nunca: ☐ Alguna vez: ☐ A menudo: ☐
9	Las dificultades se han ocasionado por:	a Ingreso equivocado u olvido de claves ☐ b Sistema no disponible ☐ c Demora en la conexión ☐
10	¿Ha socializado sus datos de usuario de acceso con alguna otra persona?	Si: ☐ No: ☐

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
MAESTRÍA EN GESTIÓN DE BASE DE DATOS – III VERSIÓN

Encuesta dirigida a los usuarios del sistema académico de la Universidad Nacional de Chimborazo

(Aplicación de preguntas con base a las cuatro secciones de la propuesta de gestión de seguridad de la información para el sistema académico de la UNACH: Gestión de activos, Regulaciones, Gestión de Incidentes, Monitoreo y Continuidad)

Marque con una X el tipo de usuario que es usted, respecto al sistema académico

Tipo de usuario	Selección
Personal Técnico	
Operador del sistema	
Docente	
Estudiante	

Lea las preguntas y marque con una X, conforme su criterio respecto a la pregunta sea afirmativo o negativo

No	Pregunta	SI	NO
1	¿Considera usted que la metodología propuesta para la identificación y valoración de activos, su monitoreo, tratamiento y mejora, permite gestionar la seguridad respecto a los activos de información del sistema académico?		
2	¿Considera usted que la propuesta respecto al marco regulatorio para la seguridad de la información que abarque no solo el cumplimiento de la norma vigente, sino que establezca políticas respecto a la organización interna, recursos humanos, activos de información, gestión de proyectos y manejo de incidentes, contribuye a una adecuada gestión de la seguridad de la información en el sistema académico?		
3	¿Considera usted que la propuesta respecto a la necesidad de contar un plan de gestión de incidentes que asegure los responsables, acciones y respuestas ante tales eventos; incide en la seguridad de la información en el sistema académico?		
4	¿Considera que la seguridad de la información del sistema académico debe ser apoyada mediante un plan de monitoreo y continuidad, que considere las responsabilidades del personal, planes de mantenimiento, capacitación, actualización de controles de seguridad y revisión de políticas de seguridad, conforme la propuesta?		